SIGNAL SECURITY IN THE ARDENNES OFFENSIVE
1944-1945

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

LAURIE G. MOE BUCKHOUT, MAJ, USA
B.S., James Madison University, Harrisonburg, Virginia, 1984

Fort Leavenworth, Kansas
1997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6 June 1997	Master's Thesis 4 August 1996 - 6 June 1997

4. TITLE AND SUBTITLE

Signal Security in the Ardennes Offensive: 1944-1945

5. FUNDING NUMBERS

6. AUTHOR(S)

Major Laurie G. Moe Buckhout, U.S. Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This thesis investigates the significance, theory and practice of tactical signal security (SIGSEC) during the Ardennes Offensive of 1944-1945. The work includes a brief introduction to the offensive and to the history of SIGSEC, and examines how the American and German armies safeguarded communications from the enemy. Inherent in this study was an investigation of actions taken by these armies to exploit their adversary's SIGSEC and the processing and exploitation of the signal intelligence (SIGINT) they obtained.

The study concludes that both armies had similar equipment, basic procedures, and training in the areas of communications, SIGSEC and SIGINT, and suffered similar deficiencies in these areas. Analysis, however, revealed a deep disparity concerning their use and importance. The Americans' near-complete lack of regard for tactical SIGINT was a major factor contributing to the success of Hitler's deception. The U.S. Army relied heavily upon intelligence gleaned from the German ULTRA code, and American intelligence officers were untrained in the use of tactical signal intelligence, mainly using it to validate operational plans. This attitude is reflected also in the American emphasis on SIGSEC. The Germans, however, were more experienced in SIGINT and SIGSEC, and formed a structure and doctrine that focused on immediately influencing tactical operations.

14. SUBJECT TERMS
Signal security in the Ardennes Offensive, SIGSEC, COMSEC, World War II army tactical communications

15. NUMBER OF PAGES
121

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	

SIGNAL SECURITY IN THE ARDENNES OFFENSIVE
1944-1945

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

LAURIE G. MOE BUCKHOUT, MAJ, USA
B.S., James Madison University, Harrisonburg, Virginia, 1984

Fort Leavenworth, Kansas
1997

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Laurie G. Moe Buckhout

Thesis Title: Signal Security in the Ardennes Offensive, 1944-1945

Approved by:

Michael J. Farley, Thesis Committee Chairman
MAJ Michael J. Farley, B.A.

Samuel J. Lewis, Member
Samuel J. Lewis, Ph.D.

Nancy A. Morales, Member
LTC Nancy A. Morales, B.A.

Accepted this 6th day of June 1997 by:

Philip J. Brookes, Director, Graduate Degree Program
Philip J. Brookes, Ph.D.

The opinion and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SIGNAL SECURITY IN THE ARDENNES OFFENSIVE: 1944-1945 by MAJ Laurie G. Moe Buckhout, USA, 121 pages.

This thesis investigates the significance, theory and practice of tactical signal security (SIGSEC) during the Ardennes Offensive of 1944-1945. The work includes a brief introduction to the offensive and to the history of SIGSEC, and examines how the American and German armies safeguarded communications from the enemy. Inherent in this study was an investigation of actions taken by these armies to exploit their adversary's SIGSEC and the processing and exploitation of the signal intelligence (SIGINT) they obtained.

The study concludes that both armies had similar equipment, basic procedures, and training in the areas of communications, SIGSEC and SIGINT, and suffered similar deficiencies in these areas. Analysis, however, revealed a deep disparity concerning their use and importance. The Americans' near-complete lack of regard for tactical SIGINT was a major factor contributing to the success of Hitler's deception. The U.S. Army relied heavily upon intelligence gleaned from the German ULTRA code, and American intelligence officers were untrained in the use of tactical signal intelligence, mainly using it to validate operational plans. This attitude is reflected also in the American emphasis on SIGSEC. The Germans, however, were more experienced in SIGINT and SIGSEC, and formed a structure and doctrine that focused on immediately influencing tactical operations.

ACKNOWLEDGMENTS

I owe a significant debt of gratitude to the many who guided me along the way. I quite simply would never have attempted nor finished this work without the encouragement of Major Mike Farley. Dr. Samuel Lewis kindly gave me the benefit of his great depth and breadth of historical knowledge and aided me in discovering that American treasure, the National Archives. Mr. Rusty Rafferty at CARL saved me endless hours of searching. Major Mike Bell provided the very framework for this thesis as well as continuous azimuth checks and proofreads, and he and his wife Terri graciously brought me into their home for hot meals and warm companionship. My father, Colonel Wayne J. Moe, USA Infantry (Retired), and my mother, Audrey Jean Soblom Moe, former First Lieutenant, Army Air Corps, have supported me unfailingly over the years, and were the inspirations for this work. I offer a special "thank you" to Paul for his loving support and gentle nudges toward completion.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

AM: Amplitude Modulation (AM):

BOS: Battlefield Operating System

COMSEC: Communications Security

DF: Direction Finding

EHF: Extremely high Frequency

ETO: European Theater of Operations

FM: Field Manual

FM: Frequency Modulation

HNW: Heeresnachtenrichtenwesens (Army Communications System)

OKH: Oberkommando des Heeres (High command of the Army)

OKL: Oberkommando der Luftwaffe (High Command of the Air Force)

OKM: Oberkommando der Kriegsmarine (High Command of the Navy)

OKW: Oberkommando der Wehrmacht (Armed Forces High Command)

RI: Radio Intercept

SIGSEC: Signal Security

SHAEF: Supreme Headquarters Allied Expeditionary Force

SOI: Signal Operating Instructions

SOP: Standard Operating Procedure

TO&E: Table of Organization and Equipment

TPS: Telegraphie par sol.(earth telegraphy)

UHF: Ultra High Frequency

VG: Volksgrenadier

VGD: Volksgrenadier Division

VHF: Very High Frequency

WNV: Wehrmachtnachtenrichtenverbindung (Armed Forces Signal Communications)

CHAPTER I

INTRODUCTION AND BACKGROUND

For many, the tremendous battle known as the Ardennes Offensive of 1944-1945 stands for a failure of Allied intelligence. This offensive, also called as the "Battle of the Bulge" for the great salient created by the enemy in the American line, has long been said to have caught Allied forces completely unaware. The Germans, considered to have been exhausted morally and economically from long years of war and heavily taxed by two fronts, surprised the Americans with a ferocious attack along the Siegfried Line through the near-impenetrable Ardennes forest, decimating entire units before being driven back amidst fierce fighting and high casualties.

Up to this point in the war, strategic and operational radio intercept indicators played a large part in the intelligence game. Once the British cryptological intelligentsia at Bletchley Park had broken ULTRA, the German code from the Enigma machine, the battle in the ether seemed won. How, then, were the Germans able to cloak an offensive of such great magnitude? Given the Allies' ability to decipher the enemy's highest level traffic and the increased awareness for communications security with which that capability must have imbued the Allies, how were the Germans able to detect U.S. Army forces with enough certainly to conduct the attack at known weak points in the American line? The answers to these question lie at least partially within the realm of tactical signal security (SIGSEC).

The purpose of this work is to examine the influence of signal security at the tactical level during the Ardennes Offensive. How did tactical American and German forces conduct SIGSEC operations and how did tactical SIGSEC affect the outcome of the battle? Secondary

questions incidental to this topic are: How was SIGSEC practiced on both sides? What were the organizations and duties of the communications and intelligence units involved with SIGSEC? How were transmissions intercepted and analyzed? To what degree was either side aware of enemy monitoring and what actions were taken to prevent it?

The answer to these questions is important not only in a historical context but because signal security is playing a key role in the planning of communications at all levels of war, strategic, operational and tactical. As communications assets have grown in capability, transmitting more data more quickly, the amount of information transmitted has expanded to fill that capability. Virtually every battlefield operating system (BOS) relies heavily on communications to pass information on intelligence, maneuver, fire support and combat support and combat service support activities such as logistics and medical support. The U.S. Army's current concept of "Force XXI" involves a flattening of echelons of command which is largely enabled by communications. Digitized perspectives of the battlefield from equipment carried by the individual infantryman could conceivably be viewed by senior battlefield planners.

As more sources inject information into battlefield communications nets, the need for speed and bandwidth grows. Terrestrial line-of-sight radio links and small-to-medium capacity digital switches will quickly be swamped. The army will not only be expanding the capacity of these existing systems and their ability to swiftly handle tremendous quantities of data, but it will also be expanding into space with the use of single channel and wideband satellite systems on frequencies relatively unused to this period, such as extremely high frequency (EHF). As this latest information revolution occurs, however, army planners must remember that just as the enemy has detected, deciphered and exploited U.S. communications in the past, he will attempt to do so again. Although the U.S. Army now uses electronic variables to encrypt communications, soldiers will still lose the electronic fill devices containing the code. Different types of

equipment still emit easily identifiable signatures: the army's Mobile Subscriber Equipment (MSE) Remote Access Unit (RAU) transmits a marker beam as distinctive as any World War II German artillery radio, and communications and cryptological equipment will still get captured.

Fortunately, lessons learned, particularly over the last sixty years, have convinced military planners of the need to protect friendly signals from enemy interception and physical compromise. However, a cognizance of necessary protection is not all-inclusive. Commanders at the tactical level, that which is defined by U.S. Army Field Manual 100-5 as "concerned with the execution of battles and engagements,"[1] do not always have the experience and background to appreciate the potential lethality of poor communications security procedures. For this reason, and because the study of lower-level SIGSEC during the Ardennes Offensive has been eschewed in favor of strategic and operational systems such as ULTRA,[2] this work will concentrate on tactical SIGSEC, that at army-level and below. An examination of past practices may convince those who would doubt the efficacy of tactical signal security and those who would disbelieve the potentially disastrous effects of ignoring it.

For perspective, this thesis examines the background of SIGSEC to World War II, and also researches German and American SIGSEC organization, training, doctrine and procedures throughout the war, narrowing its focus to the Ardennes Offensive of 1944-1945. The Ardennes Offensive offers an excellent framework in which to examine signal security. Both the Americans and the Germans have large conscripted armies and have built those armies after a period when force structures for both nations were limited to below 100,000 men. Both armies have had years during which to develop and modify doctrine and equipment, yet the Germans were war-weary and driven to use old men and young boys as soldiers, while sectors of the American line were held by units which had never seen combat. The role these factors play on

forces who should have had the benefit of years of experience adds to the complexity of the battle.

Although it was necessary to examine the entire force structure involved in the conflict, when possible this work concentrates on the two units most decisively engaged in the first days of the offensive: the U.S. First Army, and the German 5th Panzer Army. Naturally, signal security encompasses all communications means, so an analysis of enemy and friendly communications assets and procedures was necessary. This work will, however, focus on army ground force communications, although again, it includes certain germane aspects of the sister services.

As this thesis has a historical basis, I have approached my research primarily through the examination of books, unit historical reports and personal reports, transcripts of transmissions, diaries, monographs, and interviews. The U.S. Army Center for Army history produces a valuable series of great detail on a wide variety of topics. The monographs produced by senior German officers after the war, particularly those detailing German Army communications and intelligence procedures and their exploitation of U.S. Army procedures, are extremely interesting and offer a myriad of lessons that should not be allowed to settle into obscurity. General Albert Praun, the German Chief of Army and Armed Forces Signal Communication during the Ardennes Offensive, produced a very detailed monograph entitled "German Radio Intelligence (Foreign Military Studies Manuscript P-038)," which proved to be the basis for my research on the Germans. The United States Forces European Theater (USFET) General Boards produced a comprehensive set of reports on U.S. Army operations during the war, covering everything from maneuver to logistics and communications. I also have been fortunate in that my father and several close family friends served in the Ardennes and have provided first-hand accounts.

Most of the sources referenced can be found in the Combined Arms Research Library (CARL), Eisenhower Hall, at Fort Leavenworth, Kansas. Other sources were from Record Group 457 (National Security Agency) at the National Archives, which contains a great deal of material only declassified over the last decade. Unfortunately, both the Germans and the Americans destroyed many unit logs and intercept records either to prevent their capture or after the war. Therefore, any of the incidents of information gleaned from intercept are from secondary sources, but they are no less germane to the subject.

Background of Signal Security to 1944

Signals security (SIGSEC) is the denial, by various means, of friendly communications to the enemy. Vital combat communications have taken many forms, from signal fires, flags and the scribbled missive handed to a runner to teletype messages relayed for miles over wire, to the directive issued over a tactical radio net from a battalion commander. Similarly, the means of making it difficult or impossible for the enemy to intercept and understand U.S. Army communications are just as varied. Codes, which substitute one word for another, and ciphers, which substitute letters within words, have been used in written battlefield communications since the time of the ancient Greeks.

By the time of the American Civil War, General Albert J. Myer, founder of the U.S. Army Signal Corps, the first military special communications branch in history, invented an encoded signaling system using torches and flags, called semaphores, of various sizes and colors. His code was simple, consisting of only thirty-two flag movements that were called the "General Service Code."[3] To prevent the widespread knowledge of the code, Myer restricted it to officers, although it is highly likely that the enlisted personnel who operated the flags quickly learned the simple code as well. Inevitably, signal security became a problem. During the Battle of Chancellorsville in 1863, Major General Butterfield ordered flags not to be used because the

enemy could read them. The chief signal officer of the Army of the Potomac lamented that "the Corps is distrusted, and considered unsafe as a means of transmitting important messages." He added, "It is well known that the enemy can read our signals when the regular code is used."[4] Because of that, the Signal Corps subsequently introduced a cipher encryption device which consisted of two concentric disks with numbers and letters corresponding to different codes. Apparently, the enemy never broke this system.[5] The Confederates, on the other hand, continued using a slightly modified version of Myer's original code, and Union forces easily deciphered their signals.[6] It was not until later in the war, however, that field commanders trusted and understood the encoded semaphores enough to use them regularly.

The American Civil War also witnessed the extensive military use of the telegraph. Since its invention in 1844, the use of the magnetic telegraph spread rapidly and, within roughly the first decade of its use, several countries recognized its military potential. The French employed the telegraph during the Crimean War (1854-56), during which a message could be relayed over telegraph circuits from Balaclava to London in twenty-four hours. During the war, the Russians also installed telegraph lines between St. Petersburg and Sevastopol.[7] Most countries, however, did not bother to encrypt their messages, instead they used Morse code or other widely used communications codes. At that early stage, the belligerents had not recognized the value of wiretapping and they seldom targeted the telegraph wires themselves. The vulnerability of the wires to physical damage somewhat restrained total acceptance; wagons, mules and artillery frequently damaged the telegraph wires, rendering the entire system useless. Nevertheless, the telegraph opened the door to electric signaling and by the and of the nineteenth century, brought with it a greater awareness of signal security. In 1898, the United States government, realizing the U.S. Army's awareness of signal security, used the Signal Corps as censors for commercial traffic during its war with Spain. In particular, the Signal Corps

monitored telegraph lines originating from major ports that had commercial dealings with foreign nations. At the time, government regulations strictly forbid the use of codes and ciphers when communicating with foreign countries, and it was the duty of a Signal Corps officer to oversee civilian censors to enforce these rules.[8]

Other communications innovations rapidly emerged with the spread of industrialization in the nineteenth and early twentieth century, the most important being the development of the radio. In 1899, the Italian Guglielmo Marconi brought his wireless device to the United States, using it to report on the America's Cup yacht races. It was a great success, although at this time, radio only provided a medium for the transmission of Morse code signals. The U.S. Army leapt on this new development. Quick to recognize the potential of the radio, the U.S. Army also recognized its obvious shortfall: the enemy could intercept the system as easily as one's own troops. By the time of United States entry into the first World War, the use of the wireless radio had been tested not only on the ground, but in ship-to-shore, ship-to-ship, and ground and airplane to airplane configurations.[9] Military professionals accepted the fact that wired and wireless communications would be used to command and control ground and sea forces in a major conflict.[10] Again, the Signal Corps realized the security risks associated with the radio, and began to invent methods to prevent its detection by the enemy. Codes and call signs were used with the trend towards ever more sophisticated and more rapidly changing codes and ciphers.

Although cryptography had been a part of Signal Corps training since 1912, the U.S. Army did not have formal practices or doctrine for signal security. The Signal corps merely instituted specific protective measures when a particular threat seemed to warrant them. The military acknowledged the vulnerability of friendly signals as a legitimate problem, but there was still no formal means to address it.

In the absence of formal procedures, however, the U.S. Army did make advances in signal security. Often those developments accompanied or came as a result of innovations intended to improve efficiency. 1910, the Army discovered how to multiplex telegraph and telephone signals over one line, increasing the efficiency and security of the system. Additionally, in 1912 the Army adopted the International Morse code and its General Service Code, finally replacing the Myer code which had been introduced some fifty years earlier.[11] In 1915 the War Department introduced a Telegraph Code, primarily for the sake of brevity rather than security.[12]

The wartime expansion of the U.S. Army in 1917 and 1918 and the recognition that other countries had made similar technological advances in the area of intercepting communications convinced the service to consider an institutionalized method for securing friendly signals. The Office of the Chief Signal Officer for the American Expeditionary Force (AEF) in France developed a Code Compilation Section, where individuals devised the "River" and "Lake" codes for the First and Second Armies respectively. These codes were used in both wireless and wire communications, replacing the cipher disk of the Civil War which was still in use in various forms.[13] The device for the River and Lake codes, a cylinder comprised of twenty-six rotating disks, was strikingly similar to a simple but effective device used by Thomas Jefferson to encrypt diplomatic correspondence when he had been Secretary of State. To further enforce signal security, the Signal Corps fielded listening stations to monitor friendly communications for slip-ups in signal security.[14] The AEF also organized the Radio Division of the office of the Chief Signal Officer on 17 October 1917; it worked closely with the Code Compilation Section and was responsible for determining radio call signs and frequencies, which by that time could be broken down into radio net assignment and into discrete increments for the use of various units and elements.

Despite the advances in the security of American wireless communications, the radio still had limitations that could be exploited. Radio intercept, exploiting the enemy's lack of SIGSEC, became an important instrument of intelligence gathering. As early as the American Civil War, officers recommended the use of the Signal Corps for intelligence gathering.[15] In fact, General John J. "Blackjack" Pershing had a mobile direction finding and intercept team accompany him into Mexico in 1916 during the punitive expedition against Pancho Villa. The Signal corps used three mule drawn "radio tractors" to monitor enemy communications, although atmospheric conditions in the rugged terrain severely inhibited operations.[16]

The Germans had advanced along with the Americans in wireless technology, using it more extensively for communications by the outbreak of World War I. To address the enemy's use of this medium, the radio division of the AEF fielded radio sections to each field army and to AEF General Headquarters to operated intercept stations. These stations copied coded messages for dispatch back to the radio sections for deciphering. The intercept stations were able to use goniometry, or direction finding by the means of angles, to find enemy transmitters. They were able to ascertain enemy activity by the volume of traffic even when the sections could not decipher the enemy codes.[17] The stations also tapped enemy telegraph and telephone wires, and exploited the ground leaks of poorly insulated wire through a communications technology called earth telegraphy, or *telegraphie par sol,* which worked by driving iron poles into the ground to pick up electrical currents by means of electrical induction.[18]

Because of the constraints of the wireless, it was the telegraph and telephone that were the workhorses of the First World War. Indeed, the U.S. Army ran over 38,000 miles of wire and cable during World War I, although some was leased from the French. Trench warfare was ideal for wire communications, as wire and cable could be run along the same trenches in which the men were living and fighting. Communications for brigades, regiments, and divisions functioned

primarily through large switchboards, but as long as the trenches through which the wires ran were manned, the communications were essentially secure. Innovations in the wire itself contributed to signal security; the Signal Corps invented a type of wire called twisted pair, consisting of two seven-strand insulated copper and steel wires which were wrapped around one another, which eliminated the ground return wire that was so vulnerable to tapping.[19] Better insulation improved the security of these wires from ground leaks as well as tapping. The new wire, with its increased resistance to both tapping and ground leak detection, proved especially useful when employed in such area as no man's land, where U.S. Army forces could not physically secure it. By the Armistice, the Signal Corps had earned accolades for both its excellent wire communications and signal security, but the fact that the wireless had contributed so little to the war effort was a disappointment to military leaders.

The end of the Great War and the resultant cuts in U.S. armed forces during the interwar years led to a corresponding lag in the development of military communications technology. The civilian sector, however, quickly moved radio from spark-gap technology to continuous waves generated by vacuum tubes, which were capable of carrying voice and music. The U.S. Army Signal Corps remained skeptical of these advancements and channeled most of its limited funds into improvements of the telegraph. In the 1930s, the Signal Corps finally reacted to demands from the field to produce a tactical radio. Its first solution was an amplitude-modulated (AM), continuous wave set weighing twenty five pounds with a range of about five miles. In 1940, well behind the commercial communications industry and the rest of the world, the U.S. Army finally adopted frequency-modulated (FM) technology, which improved transmission distance and eliminated much of the static and noise of AM devices.[20]

The wireless dramatically changed communications on a global scale. Everyone from battalion commanders to heads of state communicated through the radio. The new medium

required no cables which could be traced, cut or tapped; on the proper frequency, signals could travel half way around the world, a very attractive feature to diplomats serving in foreign countries. The international increase in radio usage produced a corresponding rise in the concern about signal security. Now that international communications could be easily intercepted, nearly every major nation employed some sort of machine encoding or encipherment. These machines used mechanical or electrical switching or rotating devices to scramble clear messages to protect them during their passage from transmitter to receiver. The effectiveness of the machine would vary by its complexity and sophistication of the rotors. The settings were complex; if they were changed frequently and if clerks and operators did not make serious errors the enciphered messages could have a very high level of security.[21]

The Signal Corps formed the U. S. Army Signals Intelligence Service (SIS) in 1929. The SIS was responsible for the development of codes, ciphers, and cryptographic machines. It also absorbed the intelligence gathering activities previously conducted by the "Black Chamber," a covert organization within the Military Intelligence Division of the War Department General Staff which had been disbanded by Secretary of State Henry Stimson with the admonition that "Gentlemen do not read one another's mail."[22] Although the SIS had been organized primarily to train for the possibility of war, in actuality it was performing activities which were quite illegal, specifically the interception and solution of encrypted communications of foreign governments.[23]

Hitler's rise to power and the German military buildup of the early in the 1930's signaled new advances in both SIGSEC and interception and decryption technologies. As America was drawn into World War II, the SIS developed a heightened interest in encryption at the strategic level. The SIS invented scrambler phones, and early in the 1940's Roosevelt and Churchill used them to communicate, but the SIS discovered these were decipherable by the Germans. A more secure means was available by 1944 called the SIGSALY -- a ninety-ton radio-telephone system.

Obviously, it was of no use to field troops, but it provided great security at higher levels. The SIGSALY was worked by sending encoded speech over shortwave radio. Technicians on the sending and receiving end played special phonograph records that contained a secret key that masked the speaker's voice with garbled sounds. The technicians destroyed these records after each use. While the enemy monitored SIGSALY transmissions, they never decrypted them. SIGSALY pioneered technologies such as pulse code modulation and digital transmission. Its details remained classified until 1976.[24]

From 1933 to 1944, William F. Friedman, the Army's foremost cryptographer, invented a number of cryptographic machines and systems, to include the SIGABA.[25] The SIGABA, or Converter M-134-C, was a typewriter-sized encryption machine comprised of electrically powered rotors with letters of the alphabet which became a mainstay of American intelligence at all echelons. Although Americans were inventing some excellent cryptographic systems, the U.S. Army was not stressing the use of signal security in its increasing tactical training. Throughout the period of U.S. military buildup, the Germans were sharpening their eavesdropping skills on the mostly unencrypted communications of stateside American military maneuvers via long-range intercept.[26]

The United States, despite the disbanding of the "Black Chamber," still had a number of organizations besides the SIS operating independent intelligence activities, none of which assisted the others.[27] Their allies, the British, however, consolidated their assets into one of the largest intelligence organizations of any nation at the time, resulting in unified efforts in the fields of signal security and intelligence.[28] Like the Americans, the British were closely watching their enemies from the Great War. F. W. Winterbotham, the senior Air Staff representative to the British Secret Intelligence Service, wrote:

> It seemed evident that the great German war machine dedicated to the rapid blitzkrieg must have a secure and quick signaling organization, since the laying of land lines would hardly be

possible, and that the one-time cipher would be far too cumbersome and out of the question for such a volume of traffic.[29]

This inquisitive line eventually led the British SIS to the discovery of the German Enigma machine.

In 1938 a disgruntled Polish worker who had been laboring in a factory in eastern Germany found his way to a British agent, and described the machine his factory had been producing. It was a typewriter-sized system of revolving drums upon which were placed letters of the alphabet. A typewriter fed the letters of the message into the machine. The setting of the drums was the key. The British estimated that it would take a team of top mathematicians a month to run through all the possible permutations that could occur within a single cipher. Although this technology was well-known to the cryptographic world by 1938 (the American SIS had examined a machine of similar design in 1928, but had declined to purchase it), it was still a very efficient system. Germany produced thousands of these machines, which were to be used to run the Nazi war machine on individual ships and submarines, for fire departments and police and in army field units at least down to the divisional level. The Allies gave the code name ULTRA to the intelligence they were able to glean from Enigma transmissions.[30]

While British cryptologists working with the Enigma machine increasingly expanded their access to a range of German military and diplomatic codes, the Americans were working on a Japanese diplomatic code they called PURPLE. Walter Friedman and his team managed to build a replica of the machine which produced PURPLE without having ever seen one, an incredible feat. The SIS named the intelligence from this system MAGIC, and like ULTRA it proved to be of inestimable value throughout the war years.[31]

As of 1938, the SIS was functioning with a staff of eight people. These eight individuals had the mission of not only deciphering foreign codes, but ensuring the security of friendly communications at all levels. They had achieved a brilliant success with the breaking of the

Japanese PURPLE code, yet the priceless intelligence gathered from the PURPLE code was sent around the office of the Army Chief of Staff, General George Marshall, under a simple buck slip. This was later upgraded to a leather folder, but despite some astounding successes in the signal intelligence arena, the Americans seemed to be practicing signal security in a somewhat lackadaisical manner.[32] This disregard was not complete; the success of SIGSALY and SIGABA would belie that assumption. However, concern over signal security appears to be inconsistent. The reasons for this somewhat cavalier attitude at the highest levels of the U.S. Army are not entirely clear. Perhaps it stemmed from a combination of intellectual arrogance and simple naïveté, but whatever the case, the American approach to signal intelligence and signal security were to definitively impact the conduct and outcome of the Second World War.

---

[1]Department of the Army, FM 100-5, Operations (Washington, DC: US Government Printing Office), 1986, p. 1-3.

[2]I refer to the German and Japanese strategic codes of World War II such as ULTRA and MAGIC, which have been heavily researched and are very well documented in The ULTRA Secret by F. W. Winterbotham (NewYork: Dell, 1975) and The ULTRA-MAGIC Deals by Bradley F. Smith (Novato, CA: Presidio Press, 1992).

[3]Rebecca Robbins Raines, Gettting the Message Through: A Branch History of the U.S. Army Signal Corps (Washington, DC: Center of Military History, United States Army, 1995), 14.

[4]Report, Cushing to Myer, 23 May 1863, and report, Fisher to Lt. William S. Stryker, Adjutant, Signal Corps, 9 May 1863, both in War of the Rebellion: A Compilation of the Official records of the Union and Confederate Armies, ser. 1, vol. 25, pt.1, p.220 and p. 228 respectively.

[5]J. Willard Brown, The Signal Corps, USA in the War of the Rebellion (Boston: U.S. Veteran Signal Corps Association, 1896), 99-102.

[6]Ibid. At Little Round Top, they became a target of enemy fires as the Union commanders realized that the men standing on these high promontories could not only relay information, but could gather intelligence as well.

[7]Ibid., 4.

[8]U.S. War Department, Annual Report of the Chief Signal Officer, (Washington, DC: 1898), 891-95.

[9]"This development came too late to be of any substantial use at the front, but its value for peace as well as well as for any future war is obvious." Leonard P. Ayres, The War with Germany: A Statistical Summary (Washington, DC: USGPO, 1919). p. 93.

[10]The Navy was much more reluctant than the Army to allow the use of the wireless on board its ships. Captains had become accustomed to the autonomy under which they operated once at sea, and the new element of a command and control system was irksome at best.

[11]Raines, 139.

[12]John Patrick Finnegan, Military Intelligence: A Picture History, (Arlington, VA: History Office, U.S. Army Intelligence and Security Command, 1984), 32.

[13]Raines, 187.

[14]Ibid.

[15]In 1865, Chief Signal Officer Benjamin F. Fisher had recommended that the Signal Corps be used in wartime to provide communications and intelligence, collecting, analyzing and presenting intelligence reduced to "logical form" to the commanding general.

[16]Penelope S. Horgan, "Signals Intelligence Support to U.S. Military Commanders: Past and Present" (Carlisle Barracks, PA: U.S. Army War College, 1991), 14.

[17]F. W. Winterbotham, The ULTRA Secret (New York: Dell, 1974), 23.

[18]Raines, 180.

[19]Ibid., 187.

[20]Ibid., 238.

[21]Bradley F. Smith, The ULTRA-Magic Deals (Novata, CA: Presidio Press, 1992), 24.

[22]Ibid., 20. Stimson would have no qualms about reading ULTRA and PURPLE intercepts as Secretary of War fifteen years later.

[23]James L. Gilbert and John P. Finnegan, U.S. Army Signals Intelligence in World War II: A Documentary History (Washington, DC: Center of Military History, United States Army, 1993), 27.

[24]Raines, 264.

[25]Kahn, David, The Codebreakers, (New York: Scribner, 1996), 391.

[26]Albert Praun, Military Study No P-038, German Radio Intelligence, (Washington, DC: Department of the Army, Office of the Chief of Military History, 1950), 158.

[27] Smith, 26. The FBI, U.S. Army, U.S. Navy, State Department, Coast Guard and FCC were all participating in intercepting and breaking radio messages.

[28]Ibid., 18.

[29]Winterbotham, 26.

[30]Ibid., 29.

[31]Smith, 35.

[32]Ibid., 36.

CHAPTER II

AUTUMN 1944

The German Situation

Germany, September of 1944. Over the last five years, almost four million German men had died as a result of Adolf Hitler's search for *Lebensraum*. The Allied forces had invaded Normandy's beaches in June of 1944 and now controlled most of France, Belgium, and Luxembourg. The enemy was steadily encroaching towards the Third Reich's borders to the south through Italy, and like Napoleon before him, the German leader's assault on the vast land mass of Russia had foundered. What was meant to have been a lightning strike on the Eastern Front became a logistical nightmare and a prolonged war of attrition against a surprisingly determined enemy.[1] Raw materials were in desperately short supply, as the German industrial machine investigated synthetic fuels to continue to run the war.

Despite the seemingly grim situation, Hitler professed hope. There were close to ten million men still in uniform and more available, if one considered the ranks of Hitler youth, older men, factory workers, and others anxious to serve the *Vaterland.* If raw materials were no longer flowing in from those countries which now lay in the hands of the Allies, then at least excellent German technology had discovered myriad ways to overcome this. Labor was plentiful, as slave labor contributed to the effort.[2] The only thing the Third Reich needed to regain momentum was time. In Hitler's view, a tremendous German offensive could defeat at least one set of enemies, reducing the war back to one front and buying the time needed by its industrial base to produce more superior war machines that could actually turn the tide. The question was: where? Time

could be traded for space in the East. Moreover, although the Allies in the West were outrunning their own logistical support, they were still knocking on the door of the Reich. German forces were already conducting counterattacks in the west, taking advantage of the American's logistical challenges.[3] The question was settled. On 1 September 1944, Hitler convened a meeting in his Wolfschanze (Wolf's Lair) headquarters and announced to a few confidants his plans for a vast offensive on the Western Front for late November. In charge of this offensive he placed the aristocratic and battle-hardened Field Marshall Gerd von Rundstedt, who had himself just been replaced by Hitler in July for proposing withdrawal. It is here that the great deception began: Hitler told von Runstedt that he was only to defend along Germany's western border, the line of fortifications in the Ardennes also known as the Siegfried line, falling back upon it for a decisive battle to buy time for the Reich. He stressed to the Field Marshall that there was insufficient strength remaining in the Reich to mount an offensive.[4]

In actuality, what Hitler named *Wacht am Rhein*, or "watch on the Rhine" was to become known as the most stunning and audacious act of offensive maneuver in the latter part of the entire war in Europe. Hitler intended to break through a weakly held American sector of the Allied front line and retake Antwerp, isolating the British-Canadian 21st Army Group while seizing the Allied logistical center. The Sixth SS Panzer Army would be the main effort, thrusting toward Antwerp from the Monsheim-Losheim area through the Ardennes, crossing the River Meuse between Liege and Huy. The Fifth Panzer Army, as supporting effort, would thrust forward with the object of protecting the left flank of 6th Panzer Army. The Seventh Panzer Army would protect the flank of the Fifth Panzer Army, and the Fifteenth Army would cross the Meuse to link up with the Sixth Panzer Army in the vicinity of Tongres.[5]

When this plan is finally revealed to a select group of officers in the Wolfschanze on October 22, it is greeted with astonishment and skepticism by all present.[6] Hitler's staff then

proposed a "Small Solution," involving the encirclement and destruction of U.S. forces at Aachen, but Hitler completely rejected it.[7] However, largely through the efforts of Field Marshal Model, Hitler allowed some minor modifications of his plan to an offensive along a sixty-mile front in the Ardennes, with supporting attacks at Aachen to the north and Alsace to the south, although Hitler still wanted his commanders to exploit their successes and drive to Antwerp. Once Antwerp had been reached, the 21st British Army Group would be cut off, and the Allies would lose the only full-capacity port they had been able to capture. The stage for a battle of annihilation would then be set, with the Allies cut off from their supplies. Hitler estimated that it would be possible to destroy at least twenty to thirty allied Divisions.[8]

The detailed operational plan, which Hitler's staff christened "*Herbstnebel,*" or "Autumn Fog" for the conditions necessary to its success, gave the following concept: On 16 December 1944, infantry units, supported by a short but powerful artillery preparation, would break through American defenses, rapidly followed by panzer divisions. Winter's dense fog would prevent Allied air intervention and the panzer units could take advantage of the general state of confusion in which the enemy would find himself, and could establish bridgeheads across the Meuse River on the second day. The second wave of panzer units would follow and fan out on a broad front. The advance to Antwerp would resume, culminating in the seizure of the city and eventual Allied capitulation.[9] *Herbstnabel* was greeted with disgusted resignation by the Fuhrer's senior officers. As General Josef "Sepp" Dietrich, one of Hitler's most loyal subordinates and commander of the 6th SS Panzer Army,[10] stated after the war:

> I had merely to cross a river, capture Brussels and take the port of Antwerp, and all this in the worst months of the year . . . through countryside where snow was waist deep and there wasn't room to deploy four tanks abreast, let alone six armored divisions, with divisions that had just been reformed and contained chiefly raw, untried recruits, when it didn't get light until eight in the morning and was dark again at four in the afternoon, and at Christmas time![11]

Hitler's plan called for twelve panzer and panzergrenadier divisions and eighteen infantry (parachute and volksgrenadier) divisions to be committed to the attack. In fact, only five panzer and thirteen infantry divisions were in the initial assault with two more panzer divisions and a panzer brigade in support.[12] The offensive forces deployed in four Army Groups (see Appendix A for orders of battle, and Appendix B, Figures 1 and 2 for strategic maps of forces) with the main effort in the Ardennes under Army Group B commanded by Field Marshal Walter Model. Under Army Group B was the Fifteenth Army in the north, not slated to play a major role in the operation but with a supporting mission to attack North of Aachen to distract the Americans, Oberstgruppenfuhrer der Waffen-SS Josef Dietrich's Sixth Panzer Army, sharing the center sector of the Ardennes with General der Panzertruppen Hasso von Manteuffel's Fifth Panzer Army, and supporting to the south, General der Panzertruppen Erich Brandenberger's Seventh Panzer Army.[13]

The German employment of signal security was key to the success of the Ardennes Offensive. Hitler even eschewed the Enigma machine in favor of a highly disciplined program of communications silence. As the date for the offensive grew nearer, however, operational and tactical commanders transmitted many details of the operation over the wireless. In the beginning, the only indication by the more conventional communications means was on 4 September 1944 after Hitler told the Japanese ambassador to Germany, Baron Hiroshi Oshima, about a large offensive in the west to take place in November. The Baron then sent a message to Tokyo via high frequency (HF) radio using the PURPLE code, which the Americans had already deciphered. After deciphering this message, the Allies largely disregarded it, thinking the Germans too battle-weary to launch such an operation.[14] Trevor Dupuy called this lackadaisical response to the message "one of the most egregious failures ever in the history of American battlefield intelligence."[15]

Following his discussion with Baron Oshima, Hitler instituted strict secrecy for the offensive. A very limited number of people were told of his plans. All officers associated with the operation were required to sign a special pledge of secrecy, which would be violated at the cost of their lives and the lives of their families. Information regarding it was not to be passed over the wireless under any circumstances, as Hitler had rightly concluded that German radio traffic was no longer completely secure.[16] All preparations were to be conducted by land line. This was more expedient than it initially appeared, as German forces were once again at their prewar boundaries, so could now use the fixed communications infrastructure.[17]

As the use of the Enigma machine was confined to radio operations, there were no ULTRA intercepts which referred to the actual offensive to alert the Allies, although there was a great deal of ULTRA traffic requesting aerial reconnaissance and protection and logistical support in the area of the Ardennes. The fact that Allied intelligence had grown somewhat complacent, expecting ULTRA to reveal all, is highlighted by the number of other intelligence indicators that pointed to an offensive in the west that were largely disregarded: U.S. Army tactical signals intelligence was active and effective during Hitler's buildup in the Ardennes, revealing the presence and strength of units. It did not, however, reveal the operational intent of these units, but the force buildup should certainly have received more attention.[18] POWs, which were a major source of U.S. operational intelligence, spoke of an "all-out counteroffensive."[19] ULTRA and HUMINT (human intelligence) sources showed a new Panzer Army had been created in the west, and that a number of units were moving off of the defensive line in the Ardennes, perhaps to prepare for follow-on or reserve missions. These units failed to appear on Allied charts of the enemy's orders of battle elsewhere in the European theater. ULTRA transcripts told also of massive troop movements by rail to the west as Allied air reconnaissance showed convoys and trains moving in greater volume.[20] The intelligence officers at First and

Third Armies, Colonel Benjamin "Monk" Dickson, and Colonel Oscar Koch, respectively, expressed concern over such indicators,[21] but perhaps because of the absence of definitive wireless traffic expressly indicating an offensive, couched their warnings in tentative terms. General Omar Bradley, although conceding that he had earmarked specific divisions to move into the Ardennes should the Germans attack in that region, dismissed much of the information, along with that from British Major General Kenneth Strong, SHAEF intelligence officer, with a cavalier "Let them come!"[22]

For the Germans, one of the drawbacks of such an effective signals security program was the effect it had on friendly troops. As B. H. Liddell Hart wrote:

> The strategic camouflage helped surprise, but a heavy price was paid for the extreme internal secrecy. Commanders who were informed so late had too little time to study their problem, reconnoiter the ground, and make their preparations. As a result many things were overlooked, and numerous hitches occurred when the attack began.[23]

The general radio silence imposed on units moving forward in the weeks before the offensive gave new radio operators no chance to check into the nets nor to keep in practice. Radio stations further in the rear also operated under this restriction. Thus, German command authorities encountered significant difficulties in communications during the first days of the attack that they only gradually overcame.[24]

The American Situation

While Germany prepared its forces east of the Ardennes, the First, Ninth, and Third Armies of Bradley's 12th Army Group had launched attacks on the West Wall, broken the German defenses north of the Ardennes, and in fierce fighting had captured the town of Aachen on 21 October 1944. This was the first major German city to fall to the enemy, and its loss struck a tremendous psychological blow to the German people.[25] Weary from this battle and deserving a rest and a chance to refit, First Army's VIII Corps under Major General Troy Middleton was sent

to a sixty-mile front in the Ardennes, along Hitler's West Wall. This was considered "the Ghost Front," as Allied Intelligence had discounted the possibility of a major armored offensive through the densely wooded, mountainous terrain. It was already thinly held by American units and was being used as a "rest stop." Here on December 10, the 28th and 4th Infantry Divisions were joined by the newly formed 106th Infantry and 9th Armored Divisions, who had landed on Omaha Beach on December 5 and who had never been in action, although the 106th consisted of units which had trained together for the past two years. The 4th held the southernmost position from the Moselle to just north-west of Echternach. Occupying a narrow sector north of them was the 9th, and to the left of the 9th was the 28th. North of the 28th was the 106th, with its two regiments in a salient on the Schnee-Eifel. The 14th Cavalry Group held the Losheim Gap, a six-mile sector extending up to the V Corps boundary held by the 99th Infantry Division. The reserve consisted of four battalions of combat engineers and reserve command of the 9th AD.[26]

As VIII Corps moved in, the previous owners moved out, effecting almost a one-for-one exchange of battle positions. As the 38th Regiment pulled out to be replaced by the 423d Regiment of the 106th, they left the incoming units with words of caution. Colonel Wayne Moe, then commander of I Company, 423d Regiment, 106th remembers: "I had the impression they were glad to get out of there. Of course they knew the front was thinly held and they were nervous about it."[27] The outgoing commander further advised then-Captain Moe about the infamous German 88s, which were zeroed in on the U.S. fighting positions, and cautioned him against moving about too freely, as artillery and snipers were also a problem.[28]

Further preparing the positions that had been vacated by the 38th Division, the 106th dug in and waited. There were occasional probes into the American lines, which they repelled, and the Germans let loose from time to time with devastating artillery, but the soldiers had had ample time to prepare their defenses, as well as using some of the near impenetrable bunkers of the

Siegfried Line itself, so casualties were few. The evening of the 14th, I Company soldiers heard the squeaking of tank tracks and the clanking of equipment. The commander sent out a patrol, which although unable to discern specific activity through the dense woods and the dark, was able to hear even more clearly the movement of troops and equipment. Late that night, the commander again heard strange sounds in front of his sector: sounds of a locomotive, and the clanking and noise of heavy equipment. This report and those of many othr units on the front were duly reported up the chain to division and then corps level. At first the reports were dismissed as the hyper-awareness of units new to combat. The accounts of the train were brushed aside as well; there were no railroads in the area. The unit heard the sounds again and once again reported them. This time it was acknowledged that there had been a rail spur into the small town of Bleialf, but that it had long ago been knocked out by Allied air strikes.[29] In fact, the Germans had repaired this spur, and were using it to unload massive quantities of men and equipment to prepare for *Herbstnebel.*

At 0530 on 16 December the German Army cut loose a tremendous artillery barrage, cutting through the icy mist on the sixty-mile wide front to concentrate on the unlucky troops of First Army's VIII Corps. The deception had worked. It was to launch the unforgettable Battle of the Bulge, in which the Germans crashed through the U.S. lines and drove west, creating a salient over fifty miles deep. The Americans rallied in a series of sharp counterattacks, and on the 23d of December the skies cleared and Allied bombing commenced, forcing the Germans to halt their advance. On 27 December Hitler finally yielded to von Rundstedt's request to withdraw. The offensive produced some of the bloodiest fighting of the war. The Germans suffered over 100,000 casualties, and the Americans, 81,000.[30] It was to be Hitler's final blow to the West.

---

[1]Charles B. MacDonald The Battle of the Bulge (London: Weidenfeld and Nicolson,1984), 7.

[2]MacDonald, 18.

[3]Trevor N. Dupuy, Hitler's Last Gamble (New York: HarperCollins, 1994), 9.

[4]Ibid., 21.

[5]United States War Office, "The German Counter-Offensive in the Ardennes - A Study of the Initial Phases" (Washington, DC: Directorate of Tactical Investigation, War Diary Section, 18 September 1945), 2.

[6]MacDonald, 34.

[7]"German Counter-Offensive," 2.

[8]Percy Ernst Schramm, "The Preparations for the German Offensive in the Ardennes (Sep-16 Dec 44)", World War II German Military Studies, ed. Donald S. Detweiler. (New York: Garland, 1979), 12-14.

[9]Ibid., 64-65.

[10]Blaine Taylor, "A Combat History of 1st SS Panzer Division," from Hitler's Army: The Evolution and Structure of German Forces, 1933 - 1945, by the authors of Command magazine (San Luis Obispo, CA, Command magazine, 1995), 103-115. By now, of course, Hitler was almost entirely isolated from his officers. The previous summer's attempt on his life by a cabal of senior officers left him mistrustful of all but a few. General Josef "Sepp" Dietrich was one of those few, an SS officer who had been with the Fuhrer since the early thirties, when Hitler, fearing a *putsch* from either his own unruly Stormtroopers or the conservative party, ordered Dietrich to form a private guard, which became the SS. Hitler sent Dietrich and his 1st SS Panzer division into a number of engagements in which the unit would have an opportunity to excel, hoping that the German people would associate their victories with the Party and Hitler himself, rather than the regular Army. The unit became highly decorated, wearing not only military and Party decorations, but Adolf Hitler's name emblazoned on a special band about the cuffs of their uniforms.

[11]Ibid., 115.

[12]Dupuy, 19.

[13]Ibid., 8.

[14]Ibid., 12-24.

[15]Ibid., 11.

[16]Ibid., 36.

[17]Ibid., 37.

[18]Ibid., 38.

[19]MacDonald, 70. Despite Hitler's attempts to prevent news of the offensive from reaching the common soldier, preparations were so great by late November of 1944 that no German soldier could fail to see their significance.

[20]Dupuy, 3.

[21]MacDonald, 54.

[22]Ibid., 5.

[23]B. H. Liddell Hart, The German Generals Talk (New York: Quill, 1979), 277.

[24]Schramm, 243-244.

[25]Ibid., 38-39.

[26]"German Counter-Offensive," 5.

[27]Wayne J. Moe, Colonel, U.S. Army Retired. Interview with the author, Waynesboro, Virginia, 4 February 1997.

[28]Ibid.

[29]Ibid.

[30]John MacDonald, Great Battles of World War II (New York: Macmillan, 1986), 166.

CHAPTER III

U.S. COMMUNICATIONS AND SIGNAL SECURITY 1940-1941

Pearl Harbor and the entry of the United States into the Second World War caught most Americans by surprise, including the Chief Signal Officer, Major General Dawson Olmstead. One of the first challenges he had to overcome was fielding a corps of quality specialiists. The War Department's 1941 Troop Basis authorized signal troops for four field armies with associated service, photographic, repair and other specialized units. A program called the Affiliated Plan allowed the Army to draw in civilians from a variety of technical backgrounds germane to communications.[1] Unfortunately, the specialty that the Army would need the most, radio operators, were exempt from the plan so that they could be used on the home front. The Signal Corps was able to draw a disproportionately high number of its inductees from those which scored particularly high on the Army General Classification Test (AGCT) which somewhat alleviated the other induction shortcomings. Nevertheless, a service-wide phenomena became evident as troops entered combat around the world: there was simply not enough time to adequately train soldiers (or airmen, sailors or marines, for that matter), particularly in the technical specialties, before they went to war.[2] Contributing to the shortage and training challenge was the fact that the War Department mobilization plan developed in mid-1941, the so-called Victory Plan, allocated half of the Army's manpower to ground combat divisions and half to all the other supporting arms and services, essentially ignoring the technological advances of the previous two decades.[3]

It quickly became obvious that the same technological advances that prompted massive training efforts would radically change the organization of the Army Signal Corps. By 1941, the radio was playing a much larger role in the conduct of war, and the Signal Corps formed new organizations to support commanders at all echelons with communications. As global use of the radio increased, so did the interest in eavesdropping on the radio traffic of the enemy, so the SIS and the Signal Corps developed techniques and organizations to obtain signal intelligence. Signal security was also at the forefront of the SIS and Signal Corps' efforts; research conducted by the SIS was quickly translated to equipment that could benefit the tactical communicator.[4]

Organization and Doctrine

Field Manual 11-20, Organizations and Operations in the Corps, Army Theater of Operations, and GHQ, and its counterpart, Field Manual 11-10, Signal Corps Field Manual - Organization and Operation in the Infantry Division, were among those documents that established the organization and basic doctrine under which the Signal Corps would operate for most of the war. At the army level the primary command and control element for all signal forces was the Army Signal Service. As chief of the Army Signal Service, the Army Signal Officer was responsible for all signal communications aspects: wire and radio communications and frequency management, the preparation and dissemination of Signal Operating Instructions (SOIs), cryptographic operations (ensuring all code and equipment were properly distributed, used and superseded when necessary), messenger pigeons, and combat photography. He advised the army commander on issues from cryptographic security to command post locations.

In a division of labor very different from the organization of today's army, the Army Signal Officer was also responsible for collecting a great deal of intelligence products, particularly enemy radio intelligence. While the Signal Officer provided the G-2 with a constant flow of enemy order of battle information as well as details of enemy operations, he also

oversaw the counterintelligence monitoring of friendly radio and telephone nets at the army level, referring security violations to the G-2 for appropriate action. The G-2, in turn, focused the efforts of the Signal Officer in the intelligence collection process, conducted detailed analysis of the raw data, and advised the Signal Officer of enemy codes and ciphers as obtained from documents and interrogation of enemy prisoners of war. Once analyzed, all intelligence was disseminated through the G-2 to operational and tactical commanders.[5]

The Army Signal Service was authorized a headquarters section which performed many staff and planning functions, and a number of subordinate operational units to include two signal battalions, construction, which were responsible for the radio and wire communications for the army headquarters. In addition, there was a signal company (photographic), a pigeon company, a signal radio intelligence company, and a depot signal Company.[6] (See Appendix B, Figure 3 for an organization chart of the Army Signal Service).

Contrary to popular belief, pigeons were not outdated relics of antiquated First World War communications; indeed, they had proven to be reliable when newer technologies failed, and they were bred and trained through the entire war. The signal corps established lofts from army to corps level, with distribution of the feathered messengers made to lower levels (often divisional signal companies, which integrated them into the message center) in mobile pigeon lofts. Shotguns organic to the pigeon company were employed as a unique means of active Signal Security; they were used to shoot birds of prey. In addition, the unit was authorized pigeon protective bags to protect the birds against gas, and baskets to deliver them to combat units.[7] Pigeons, however, were only intended to deliver unclassified traffic; they could deliver confidential and secret traffic only when no other communications means was available. In addition, unit SOPs specified that the birds would always be released in pairs, one carrying the

original message and one carrying a duplicate. Bad weather, darkness, and the enemy all reduced the chances of the birds arriving safely back at their home loft with the messages.[8]

As well as administrative, supply and training sections, the headquarters element, Army Signal Service, had a communications section, responsible for plans and studies for message traffic handling and overall network management to include frequency allocation, and employment of the two signal battalions and the pigeon company. It also had a signal intelligence section, which had an enemy code and cipher section, a goniometric (direction finding) section, and a communications security section. The signal intelligence section had the responsibility to supervise the employment of the radio intelligence company and analyze the information it obtained, preparing and recommending issue of Signal Operating Instructions (SOIs), cryptoanalyzing enemy codes, ciphers, and messages, and recommending communications security measures to ensure security of friendly signals. The radio intercept company was to obtain information on friendly signal security violations. Finally, the signal intelligence section was to maintain "intimate contact" with the G-2 of the army.[9]

The Signal Corps formed the signal radio intelligence (RI) company at army and theater level. The RI company was responsible for locating enemy radio stations and intercepting enemy radio transmissions, but its duties also included the monitoring of friendly communications to watch for breaches of security. The introduction of signal information and monitoring (SIAM) units in 1944, specifically tasked to monitor friendly communications both to identify breaches of security and to keep the commander current on friendly unit operations, supplanted the requirement for RI companies to monitor friendly nets.[10]

The Signal Corps organized signal radio intelligence companies at both theater and army level and could field twenty stations which normally operated in sections of four stations each. Each of the three operating platoons had one intercept station and four direction finding stations.

The headquarters platoon had two intercept sections. Three sections consisting of four intercept stations each would generally perform intercept activities at the army level, and the other two sections, also of four stations each, would often be attached for service to subordinate units of the army. The combined number of twelve DF stations were to operate on a doctrinal army front of approximately thirty-five miles.[11]

Each platoon in the RI company also had a control section which passed on target and mission information to the position finding section, plotted the azimuths, or lines of bearing (LOBs) from the position finding stations, and plotted the data on a map to determine the location of the enemy transmitter. One LOB result determined the general arrival direction of the signal. Two bearings from the same signal resulted in a "cut." Three LOBs from three or more different stations were required for a "fix"[12] or a definite location, which the control section would plot and collate before forwarding back to company headquarters and back to the Signal Intelligence section at army and theater.[13]

Doctrinally, intercept stations performed both search and guard missions: either to constantly roll through the spectrum to find enemy transmissions or to "watch" a specific frequency. Information gleaned from those activities included not only station identification and frequency, but also the character, mode and strength of signals; the speed, time and schedules of transmission; personal characteristics of observed operators and other identifying information. A daily goal was to identify army, corps and divisional nets. Once those were pinpointed, it was a much simpler matter to deduce the enemy order of battle. Order of battle identification was particularly easy if the enemy operators transmitted even intermittently in the clear. Even if the enemy practiced excellent signal security, the transmissions alone had many uniquely identifying characteristics. The intercept section would pass this information on enemy stations through the

control section to the position finding section, giving it additional "targets." (The doctrinal organization for the signal radio intelligence company is illustrated in Appendix B, Figure 4).

At army level, the communications responsibility was divided between two signal battalions. Each had a headquarters and headquarters company which handled training and administration, a construction company, charged with heavy and light wire construction, and the operations company. The operations company had a messenger center responsible for sending and receiving teletype messages and continuous wave (CW) messages, a messenger platoon of air, motor and foot couriers, a wire operations platoon, a wire installation and maintenance platoon, and a radio operation and maintenance platoon. The operations company also handled overall coordination for communications missions.[14]

The corps level signal structure was functionally similar to that found at the field army, but the corps depended on an army signal battalion for photographic, radio intelligence, code and cryptography, and pigeon assets. One signal battalion was assigned to each corps, with the battalion commander, either a major or a lieutenant colonel, acting as both the battalion commander and the corps signal officer. As at army level, the signal battalion fielded a headquarters and headquarters company, a construction company, an operations company and attached medical personnel. The construction company installed and maintained all types of wire circuits required by the corps, and the unit could perform both light and heavy wire and cable construction, including setting up telephone poles and stringing cable and wire.[15] The emplacement of cable on poles or trees, called "overheading" it, accomplished several objectives: it reduced the chance of damage from artillery and vehicles, it separated communications cable and wire from power cable, which could create interference, and it prevented ground-wave signal leaks which the enemy could intercept and exploit. (See Appendix B, Figure 5 for an organization chart of a corps signal battalion).

The operations company of the corps signal battalion was responsible for message center operations but had no organic troops for messengers; it usually depended on the corps quartermaster service or other units to supply messengers. The operations company also contained a radio platoon and a wire platoon. The wire platoon was responsible for the internal wiring of the corps headquarters. The radio platoon installed, operated and maintained the corps headquarters radio nets. A corps would usually operate one station in the army command net, one in the corps command net, and two vehicular stations, one of which operated in the corps reconnaissance net.[16] The other would be tasked to operate on an as-needed basis. In addition to those nets at the corps headquarters, there were reconnaissance, antiaircraft, artillery observation, and artillery air-ground nets. Units could, by shifting frequency, enter similar nets at army or division.

The communications organization in ground combat divisions consisted of a single signal company. The division signal company provided three platoons: an operations platoon with a message center (with organic messengers), a radio section, and a telephone and telegraph section; a construction platoon, which provided for the laying of heavy and light cable; and a radio intelligence platoon. The RI platoon could field three intercept teams, three direction finding teams with a plotting team, and a control section. The platoon could provide DF and intercept service to a division front.[17] Doctrinal organization charts from Field Manual 11-10, Signal Corps Field Manual - Organization and Operations in the Infantry Division, show the RI platoon leader falling under the company commander, but with a reporting line directly to the G-2. That relationship, however, is not as odd as it might sound, particularly since the commander would have been focused on friendly communications issues.

Signal Security

At all levels, from the platoon through the theater headquarters, cryptographic machines, codes and ciphers were an integral part of World War II operational and tactical communications. William F. Friedman (see Chapter 1) and others with the SIS[18] struggled to design effective cryptographic machines while simultaneously attempting to break those used by the enemy. The most widely used method of machine cryptography operated on the wired codewheel or rotor principle, and could be either electrically wired or manually set.[19] The various versions of the German Enigma machine were of that design, as was the American top-level SIGABA, also called the M-134-C. The SIGABA was perhaps the most mechanically and cryptographically complex wired rotor machine in use and provided excellent communications security.[20] The SIGABA encrypted wired teletype transmissions and radio transmissions down to division level.

The M-209 cryptographic machine served from the army level down to battalion. The M-209 was based on a 1934 design by Boris Hagelin, which was later refined for use by the U.S. Army. The M-209 was very small and thus well suited for field encryption, measuring only 7 inches by 5½ inches by 3¼ inches in its olive drab metal case. Within the case were twenty-seven bars arranged in a horizontal revolving cylinder. The bars had projecting lugs which struck "guide arms" or vertical rods, which were controlled by six key wheels upon which were printed the letters of the alphabet. For successful encoding and decoding, the lugs and pins needed to be identically set on both machines. The sender would turn the wheel to get a random set of six letters, which would be included in the text of the message in a prearranged location so the receiver would set his machine to the same combination. To read a received message, the user would twirl a knob at the left of the plain text letter and revolve a handle at the right. The mechanism spun and a little typewheel printed the output on a gummed tape. In the case came extra tape, oil for the gears, ink pads, tweezers and screwdriver. It weighed only six pounds and

could operate in temperature and humidity extremes from the Ardennes to Tunisia.[21] Although enemy reports indicated that this device offered mediocre security, its ease of use and reliability in all climates overcame any hesitation in the field. (See Appendix B, Figure 6 for an illustration of the M-209.)

At the corps level, the M-209 and SIGABA were both used, as well as map codes and call signs. At division level, the same complement of M-209 and SIGABA remained, but units used more map codes, call signs and other specific codes that were printed in the SOI in order to communicate with subordinate units lacking mechanical cryptography.[22] Early in the war, lower echelon units also used the M-94 encryption device, first issued by the U.S. Army in 1922. Designed by an eminent cryptologist named Parker Hitt, it strung twenty-five aluminum alphabetically lettered disks the size of a silver dollar on a spindle four and one-quarter inches long. These were spun in prearranged positions to encode and decode messages. In the late 1930's the Army migrated to a variation of another device designed by Hitt, the M-138-A. The M-138-A, also called the "strip system," was used concurrently with the M-94 for a period, and then replaced the M-94 by the war's end. It improved upon the M-94 by providing 100 slides, 30 of which were used at a time. So long as the strips were kept secret and changed often, the device was secure. In fact, it was discovered after the war that the Axis never deciphered the M-138-A. Hitt had designed the strip system by printing a plain and mixed alphabet twice on several paper strips, numbering them, and arranging them in a holder in an order given by a keynumber. To encipher, he slid the slips up or down until they spelled out the first twenty letters of the message in a horizontal line and then selected any other line as the cipher text. This was repeated until the entire message was enciphered. This system was converted to a wheel form to make the M-94 and M-138-A.[23]

The Navajo tribe was another interesting cryptological resource investigated and employed by the Signal Corps. Although Comanches participated in war games, it was the Navajo tribe that eventually contributed over four hundred "code talkers" to the war effort. The SIS estimated that only twenty-eight non-Navajos knew the language - an extremely complex one - and these were non-German, non-Japanese missionaries or anthropologists. Although the codetalkers were extremely effective, and the enemy never broke their language, they were primarily used in the Marines Corps.[24] Few served with army units, and those that did were in the Pacific and not in the European and Mediterranean theaters.

All levels of command employed Signal Operating Instructions, or SOIs, to set policy on a number of communications issues. In addition to the operating instructions the title implies, the SOI sometimes included one-time pads (a system using unique sheets of code which were used only once for each transmission and then destroyed), code sheets which gave code names to commonly used words, sometimes as many as five thousand to a book, and call signs and frequency lists. The printed codes were particularly valuable for those lower-echelon units that had no machine encryption assets (company, platoon, and sometimes battalion). SOIs usually included the following types of information: twilight, sun and moon charts; timing of messages; messenger service (pickup and delivery times, locations and serviced units); phonetic alphabet and numeral pronunciation; authentication procedures; radio procedures, frequency allocations and radio security procedures; telephone code names and procedures; teletype call signs and procedures; and visual signal procedures such as lights, pyrotechnics and aircraft panels.[25]

Equipment

Radio had the potential of freeing the combat commander from the confines of an immobile, fixed command post. General Alfred von Schlieffen's vision of a fixed command "suite," miles from the din of the front, where the commander could receive telegraph and

telephone communiqués, had little appeal to many modern commanders, particularly those involved with mechanized, mobile forces.[26] Although the radio still allowed commanders to quickly contact subordinates, at higher echelons however, U.S. Army command posts remained too large and unwieldy to move quickly. Indeed, it was and still is common at the army, corps, and even division level for commanders and their staffs to take over buildings, depending on their situation, temperament, and their unit's activities.

The emplacement of very large command posts or those of a unit in the defensive or in a stable situation allowed the extensive use of wire and cable. There were two reasons for that trend: the first was for security reasons, as radio was so easily intercepted and located, and once located, a command post could be destroyed by the enemy, and secondly, the number of wire lines that could be installed far outstripped the number of available radio nets, allowing more people to send and receive information. For all of these reasons, U.S. Army doctrine encouraged the use of wire at command posts and by subordinate units. For instance, it was policy for combat units down to platoon level to employ W-110 field wire and EE-8 field telephones when in the defense or in a stable situation.[27]

The EE-8 field telephone was a tough, battery- powered piece of equipment with a design unchanged since the early 1930s - small, light and effective. It was connected by field wire to tactical switchboards with considerably less to offer: the BD-71 (six lines), BD-72 (12 lines) and the BD-14 (40 lines) which were modification of French units used in World War I. The BD series of switchboards were heavy, used storage batteries, and required the caller to crank a handle in order to ring the switchboard operator, who in turn cranked in order to ring the telephone of the person being called. Technicians and customers alike deemed the central office switchboards for use at larger headquarters, the TC-2, TC-3 and TC-4, good pieces of equipment, but their permanent truck installation limited deployment.[28]

Units in the offensive or highly mobile units did not use wire extensively simply because it takes much more time to install than radio networks. Because reconnaissance elements such as cavalry and aviation, and motorized and mechanized units were too mobile to efficiently use wire, they depended on radio communications extensively. Wire and cable also needed to be recovered for re-use, and during rapid command post displacements this was not always possible. W-110, rubber insulated two-strand copper and steel wire, and W-130, which consisted of two strands of W-110 twisted about one another, called "spiral-four," were expensive and difficult to obtain through resupply.

The Signal Corps was finally becoming part of the wireless revolution that had sped around the globe. In 1935, the U.S. Army fielded the SCR-194, or "walkie-talkie," an amplitude modulated (AM) transceiver with a range of up to five miles. Manufactured for front-line tactical units, it weighed only thirty-five pounds and was designed to be carried on a soldier's back. This was a radical change in communications; commanders could now reach units that had outrun field telephone lines.[29] Frequency Modulation, or FM, however, had just been introduced to the communications industry. FM eliminated much of the noise and static interference of AM and could transmit a wider variety of sounds. When used with crystal controls, it could be tuned much more quickly and precisely,[30] and that precision tuning allowed for more efficient frequency use in a given spectrum.

For a variety of reasons to include the AM-oriented communications industry's resistance, the Signal Corps did not capitalize on FM until late 1940. In 1941, the Signal Corps converted the SCR-194 to FM, and it became the SCR-300 which served combat units until the end of the war.[31] Although the Signal Corps had fielded an improved FM radio for forward troops, the SCR-300 could not communicate with the squad-level hand-held handy-talkies, a small AM radio weighing five pounds, nor could it communicate with the FM tank radios in the

500 series, as the frequency ranges did not overlap.[32] To make communications more difficult, the artillery had adopted incompatible FM radios of different frequency bandwidths in the 600 series for heavy and medium artillery fire control purposes.[33] Another drawback of the SCR300 FM walkie-talkie was that it required a skilled trained operator who could change its crystals.

For the U.S. Army, radio telephone and radio telegraph provided the mainstay of long distance communications in theater from army through division. The SCR-299, an AM radio designed as a radio telephone, became a workhorse at echelons from Army down to division. It had a range of 100 miles, was vehicular mounted, and could be operated in a fixed or mobile configuration. Along with its close cousin, the SCR-399, it became the mainstay for long-haul communication, with a range of up to 2,300 miles when operated as a radio telegraph.[34]

The Signal Corps made considerable advancements in the years between the two world wars, particularly in the arenas of cryptology and radio. World War II, however, would be a tremendous proving ground, as demands from the battlefield forced the development of better technology. Despite the advantages of the new technologies and equipment, problems with communications security, compatibility, and reliability persisted throughout the war. Furthermore, for the Signal Corps, organization and manpower deficiencies remained not fully resolved. Almost four years would pass before the Germans would launch the offensive in the Ardennes; lessons learned would force considerable change upon the doctrine of 1941.

---

[1]Raines, 255.

[2]Ibid.

[3]Charles E. Kirkpatrick, An Unknown Future and a Doubtful Present: Writing the Victory Plan of 1941 (Washington, DC: Center of Military History, United States Army, 1990), 103-106.

[4]By 1941, the SIS had grown from eight employees to over three hundred. It was to mushroom again to over ten thousand employees, both military and civilian, by V-J Day.

[5]First U.S. Army, "First Army Combat Operations Data" (Governor's Island, New York: Headquarters, First Army, 18 November 1946), 167.

[6]United States. War Department, FM 11-20: Signal Corps Field Manual - Organization and Operations in the Corps, Army, Theater of Operations, and GHQ (Washington, DC: War Department, 1940), 28.

[7]Ibid., 21.

[8]European Theater of Operations, United States Amy, "Signal Operating Instructions Index No 1-20," ETOUSA, 14 February 1945.

[9]FM 11-20, 35.

[10]National Archives, File SRH 228, "Histories of Radio Intelligence Units, European theater, September 1944 to March 1945." (Washington, DC: Records of the National Security agency, National Archives Records Group No 457 - hereafter referred to as NA RG No 457 - 1 February 1946), 120.

[11]FM 11-20, 47.

[12]Jeffrey S Harley, "Reading the Enemy's Mail: Origins and Development of U.S. Army Tactical Radio Intelligence in World War II, European Theater of Operations" (Fort Leavenworth: U.S. Army Command and General Staff College), 109.

[13]FM 11-20, 49.

[14]Ibid., 4-9.

[15]Ibid.

[16]Ibid., 14.

[17]United States. War Department, FM 11-10: Signal Corps Field Manual - Organization and Operations in the Infantry Division (Washington, DC: War Department, 1941), 2.

[18]The SIS was to change its name several times throughout the war, adopting the moniker of the Signal Security Agency in July 1943, a name which lasted until the end of the war.

[19]For an excellent description of the development of rotor-based cryptographic machines, see David Kahn's The Codebreakers (New York: Scribner, 1996), pages 411 to 427.

[20]Cipher A. Deavours and Louis Kruh, Machine Cryptography and Modern Cryptanalysis. (Dedham, MA: Artech House,1985), 10.

[21]Kahn, 425-432.

[22]Twelfth U.S. Army Group Survey, SRH-48, Subject: The Use of Codes and Ciphers During Critical Operational Period, (Washington, DC: Records of the National Security Agency, NA RG No 457).

[23]Kahn, 325.

[24]Ibid., 550.

[25]European Theater of Operations, United States Army, Signal Operating Instructions Index No 1-20 (ETOUSA: 14 February 1945).

[26]Martin van Crevald, Command in War (Cambridge: Harvard University Press, 1985), 153.

[27]Moe.

[28]David L. Woods, A History of Tactical Communications Techniques (New York: Arno Press, 1974), 201-202.

[29]Raines, 230.

[30]Ibid.

[31]Ibid., 277.

[32]Ibid.

[33]Ibid.

[34]Ibid., 292.

CHAPTER IV

THE ARDENNES OFFENSIVE: THE AMERICANS

By the time the U.S. Army reached the European continent in June 1944, it was considerably different than the army for which doctrine had been written in 1940. Combat experience allowed the Army to envision new operational requirements, Meanwhile, both civilian and military research agencies were labored to equip newly created units and refit old ones. The demands of mobile warfare led to the creation of new radios of better range and reliability. Increasingly since 1940, cryptographic equipment and procedures were defined and in some cases, simplified, and most field communications equipment was smaller, lighter and "toughened" to meet extreme field conditions. Experiences in the Pacific, in Africa and in Italy had taught the Americans the importance of safeguarding friendly communications and the value of intercepting those of the enemy. As a result of these oft-painful lessons the U. S. Army determined that some assets such as signal interception and direction finding units were of insufficient quantity to meet actual wartime demands. To correct that deficiency, the Signal Corps created signal information and monitoring (SIAM) units were created to monitor friendly transmissions for transgressions and violations of signal security. Experience also resulted in the solidification and formalization of the roles of the signal officer and links between the signal and intelligence communities at different echelons.

In the European Theater of Operations, United States Army (ETOUSA), the First U.S. Army's signal officer, Colonel Grant Williams, was responsible for all signal communications within the army's area of operations. In 1944, signal communications included an array of

operations and tasks such as wire and radio communications and frequency management, the publication and dissemination of Signal Operating Instructions (SOIs), cryptographic operations (ensuring all code and equipment were properly distributed, used and superseded when necessary), messenger service to include those carried by pigeons, and combat photography. (See Appendix B, Figure 7 for an organization chart of First Army Signal Service). Colonel Williams advised the First Army commander, General Courtney Hodges, on issues from cryptographic security to command post locations. During one command post relocation, General Hodges was asked when he intended to move the headquarters again. Hodges replied, "I do not know. I never move anywhere until Williams tells me I can."[1] Per contemporary doctrine, Colonel Williams was also responsible for a great many activities now solely under the bailiwick of the Military Intelligence Corps, such as the collection of enemy radio intelligence and counterintelligence monitoring. While the army signal officer provided the G-2 with a constant flow of enemy order of battle information, as well as details of enemy operations, he also ensured the monitoring of friendly radio and telephone nets at the army level, referring security violations to the G-2 for appropriate processing. The G-2, in turn, advised the signal officer of enemy codes and ciphers obtained from documents and interrogation of enemy POWs.[2]

An important figure in army level communications and signal security was the G-2, a position filled at First Army by Colonel Benjamin "Monk" Dickson. A man with a reputation as a pessimist and an alarmist, it was not unusual for him to place an enemy unit on the Western front after learning that the Russians had lost contact with it in the East. Dickson also operated in a rather unique fashion when it came to special intelligence obtained from ULTRA - the product of the German Enigma machine. By late 1944, British intelligence analysts at Bletchley Park were sending decrypted ULTRA messages via special circuits to more than fifty Allied headquarters, down to army level. A very small, select staff of individuals grouped in special

liaison units, or SLUs, was on hand at each location to receive these documents. Normally, the head of the SLU would then brief the commander, and the commander only. In Dickson's case, he insisted on presenting the ULTRA brief to the commander himself, excluding Lt. Col. Alfred G. Rosengarten, Jr., his SLU chief.[3]

American intelligence officers of the era, almost to a man, did not have a particularly high standing in the officer ranks. Military Intelligence as a separate branch of the army did not yet exist, so officers often were "drafted" into S-2 and G-2 positions by such discriminators as a special knack for languages, as displayed by Dickson, or in the case of General Edwin L. Sibert, Bradley's G-2 at 12th Army Group, a tour of duty as an attaché.[4] At battalion and regimental level, the officer who was unfit to command for one reason or another often became the S-2, although many fine officers distinguished themselves in these positions.[5] General Sibert stated he had frequently overheard others say of him: "I wonder what is wrong with him that he is in G-2."[6]

Colonel Dickson was rumored to have had a strained relationship with General Sibert, reportedly jealous of both the rank and position that he regarded as rightly his own. Rather than meet with Sibert, Dickson preferred to rely on intelligence from the 21st Army Group when he needed counsel from a higher command.[7] Colonel Dickson's attitudes also served to undermine the constant liaison necessary between First Army's signal intelligence organizations and Signal Security Detachment "D," the SIS organization at 12th Army Group responsible for the coordination of all signal intelligence activities within the army group.

As well as training, supply and administrative sections, Colonel Williams' staff had a communications section responsible for all wire and HF and VHF radio communications, a message center including an air messenger squadron, a pigeon company, and a signal intelligence section. The signal intelligence section was responsible for the maintenance of all codes,

including the compilation of various code and cipher keys for low and medium grade traffic, operations of the army SIAM company, the army radio intercept company, and the tasking and mission for the subordinate corps signal service companies.

The organization at First Army differed slightly from that delineated in FM 11-20. The responsibility for SOIs shifted from the SIS to the training section, and the communication security section disappeared. To facilitate communications operations, FUSA organized a communications control office, a section not authorized under FM 11-20, It was manned by the signal officers of the 17th Signal Operations Battalion and the 32d and 35th Signal Construction Battalions and monitored all phases of communications work. The control office had the ability to reroute circuits, patch out defective facilities, and dispatch troops where necessary to ensure communications.

Another significant doctrinal improvement appeared which, if fully implemented, may have enabled the First Army signal intelligence section cryptographic team to concentrate primarily on friendly codes and ciphers: intelligence teams were finally included in the army and subordinate corps radio intelligence units to conduct analysis of low-level traffic. This action was intended to solve the many problems associated with retaining all analysis functions at the army SIS level: timeliness of decode and the rapid dissemination of useful information suffered, and without guidance from knowledgeable intelligence specialists, intercept and DF operators often wasted hours on less lucrative targets.[8] SHAEF, however, established a policy which allowed only German messages enciphered in lower-level cryptosystems, which the Allies called PEARL, to be solved below army level. PEARL consisted mostly of jargon codes, simple substitution ciphers and transposition systems emanating from units at regimental level and below and was fairly easily solved,[9] but once solved, the decrypts still had to filter through the G-2 office before they were disseminated to tactical units. RI units had to send traffic from medium-

level systems, called CIRO PEARL, to Army SIS.[10] Because of this directive, timeliness doubtless suffered and the intent of decentralization was at least partially defeated. In one case, CIRO PEARL messages were intercepted on November 6, 1944, but were not decrypted and translated at First Army until November 11, 1944, whereas PEARL messages were deciphered by the next day by lower level units.[11]

By 1944, the Signal Corps had finally recognized that the corps also needed to have RI assets, so it formed signal service companies in the European Theater, primarily from a nucleus of the radio intelligence platoons in the divisional signal companies[12] with an organization based on a TO&E developed by the First Army.[13] Five signal intelligence units supported Fist Army: the 113th Signal Radio Intelligence Company at the First Army and the four numbered signal service companies at supporting each of the subordinate corps: 3259th in support of III Corps, 3250th in support of V Corps, 3251st supporting VII Corps, and the 3254th in VIII Corps. In addition to conducting intercept and direction finding operations, the 113th coordinated missions among those corps units.

The signal service companies were generally organized with a company headquarters team, two platoon headquarters teams, one radio intelligence platoon with a traffic analysis section, two radio intercept teams, one radio direction finder team, a message center and a teletype team.[14] They were roughly half the size of the army-level unit, with 129 men authorized in each.[15]

Both the corps and army level RI units had German-speaking operators to intercept German voice traffic, but sometimes a dictaphone was used as well to catch every word. The units kept files on units, personalities, code names and call signs; the fact that the Germans used a fixed call sign system until November 1944 was extremely beneficial to American units. In addition to the intercept section's files, more enemy information was maintained by the DF

section in the form of enemy order of battle overlays.[16] As stated above, mid- and high-grade code had to be forwarded up to army for decryption and analysis, but if the signal service company traffic analysis officer found low-grade code to be of immediate tactical value, it was immediately sent to the corps G-2 for evaluation and if deemed appropriate, dissemination to affected units.

The SIAM units referenced earlier were created by the Signal Corps to relieve the signal RI units of the responsibility of monitoring friendly transmissions for security transgressions, a requirement not envisioned in 1941. The Americans first used SIAM units in the Italian campaign, modeling them on the British "J," or intercept service, which had been developed in the British Eighth Army in North Africa. Not only were SIAM units valuable in monitoring friendly communications, both wire and wireless, but they also provided staffs of division, corps and army with prompt tactical information. This, in fact, became the SIAM units' primary duty. In a fluid tactical situation where smaller units were displacing rapidly, commanders were often unable to update their higher headquarters through normal channels. In several cases, SIAM information on friendly units kept them form being shelled by friendly artillery. SIAM units also provided divisions with much of the information on units on their flanks and activities elsewhere on the front.[17] The following is a prioritized list of friendly information requested by the army staff from a typical SIAM unit: the location of leading elements of battalions and the areas covered by cavalry squadrons, the locations of corps and division command posts, the locations of combat commands of armored divisions, the intentions of divisions and regiments, and any information concerning the identification of new German units, prisoners of war totals for not less than twenty-four hour periods and any other unusual or important information which would be of value to the army G-2.[18]

In order to provide the required information, SIAM unit personnel handled incoming data in the following manner: Traffic was received and logged in by the radio operator, further logged and deciphered by the code clerk, and then checked, screened and plotted on the company operations map by the SIAM staff officer on duty. The SIAM officer then passed the traffic on to the teletype operator who gave the message a daily reference number and transmitted it to the army SIAM operations room. Once received at army, a SIAM duty officer plotted it on the army SIAM operations map , and the required number of copies were typed and distributed to the army staff.

The SIAM unit at army level used monitoring teams to operate at subordinate corps and divisions. The teams used radios compatible with the type of unit they supported: thus, armored division teams used SCR-399s to listen in on armor nets. The platoon leader for each team carried a "letter of introduction" to the subordinate unit commanding general that explained the team's duties and liaison activities with each staff section. SIAM units used radio, messenger and teletype to coordinate with their army headquarters and generally displayed excellent signal security awareness. Policy dictated that no traffic would be transmitted in clear text over SIAM radio nets, so all messages to include routine administrative details, were enciphered by a one-time pad, which offered the best cryptographic security but was slow and subject to errors.[19] (See Appendix B, Figure 8, for an organizational chart of the army-level SIAM service.)

Communications

Although the issues of tactical survivability, training of personnel and adequate supplies and equipment posed genuine problems, for the Signal Corps the most important aspects of wireless communications were the development of equipment with increased range and smaller size.[20] It was noted that by the time of the Ardennes offensive that: "from corps downwards to company

headquarters it became possible, even though not desirable, to depend on wireless entirely for extended periods of operation."[21]

The Americans realized significant improvements in communication at the army level with the introduction of multichannel radio--no longer did the commander and his staff have to rely upon single-channel radio nets or wire for communications. By the time of the Ardennes offensive, the Signal Corps had developed the AN/TRC (for Army-Navy Transportable Radio), a long-range VHF multichannel system that provided several duplex speech and teletype circuits at either end. The carrier systems consisted of two terminal sets and three intermediate relay sets to be placed twenty-five miles apart.[22] It could be quickly taken on and off a truck or trailer and was more difficult to intercept, allowing the 12th Army Group to communicate with First Army and subordinate divisions. AN/TRC integrated radio and wire together, allowing a radio transmission to a receiver, then to a switchboard, then over wire to a telephone. Pictures, drawings and typewritten text could also be transmitted by facsimile. This technique allowed the 12th Army Group to communicate with First Army and subordinate divisions. General Bradley called the telephone system the "most valued accessory of all"[23] and later commented:

> From my desk in Luxembourg I was never more than 30 seconds by phone from any of the Armies. If necessary, I could have called every division on the line. Signal Corps officers like to remind us that 'although Congress can make a general, it takes communications to make him a commander.' The maxim was never more brilliantly evidenced than in the battle for the Ardennes.[24]

Other innovations were less sweeping and were sometimes no more than unit level "tailoring" of issued equipment to meet specific needs. For instance, in order to keep in touch with rapidly moving armored units, the First Army had devised mobile communications centers mounted in vans to enable command posts to move more swiftly. The impetus for that innovation is not clear, but it was probably an attempt to imitate the signal equipment that the German Panzer Army in Africa had used to such good effect in the Libyan Desert and Tunisia.

Below division level, technological improvements were not particularly dramatic: although the Signal Corps had fielded an improved FM radio for forward troops, the thirty-five pound FM SCR-300, many units at company level did not have radio operators to assist with the complicated exercises of changing batteries and crystal-tuned frequencies.[25] The SCR-300 could also still not communicate with the squad-level hand-held "handy-talkies" or the FM tank radio, the SCR 399. That drawback caused great difficulty in tank-infantry team communications as leaping on the back of a tank to coordinate movement in battle was a risky business at best.[26] First Army signal troops attempted to fix this by giving SCR-510s to the infantry troops to carry, but when the going got rough, the foot soldiers would abandon the heavy sets. Finally, just before the Ardennes offensive, they placed light-weight SCR 300s in the turrets of some lead tanks. This provided better communications, but added to the discomfort of the already cramped crew.[27] Of course, the terrain of the Ardennes was not conducive to radio communications of any sort that the era could offer. In general, however, the clarity of American FM radios enabled soldiers to communicate clearly over the din of artillery and tanks, prompting one infantry battalion radio operator to write: "FM saved lives and won more battles because it speeded our communications and enabled us to move more quickly than the Germans, who had to depend on AM."[28]

American communications along the Ardennes front consisted mostly of wire and captured German switchboards. The Germans built the switchboards of light-weight plastic; they terminated from eight to ten tactical telephones and were simple to use. They were far superior to the heavy American BD-71s and 72s. The Americans used a mix of American and German field telephones with these switchboards, and ran wire along the front to connect battalions down to companies and further down to platoons. The wires were strung overhead in the trees to protect them from the frequent artillery barrages that would probe the front.[29] From battalion to

regiment and higher the Signal Corps used the larger U.S. Army switchboards. The use of wire in the defense, of course, rendered German wireless interception ineffective.

Shortages and problems with communications equipment began with D-Day and continued throughout operations in the ETO. Salt-water soaked radios in the Normandy landing had to be repaired by tinkering officers as trained repair troops were not available, much of the equipment was not ruggedized, and supply problems prompted the statement, "No two tanks arrived with exactly the same amount of equipment."[30] In the early planning stages of D-Day, most equipment came over marked for a specific unit. However, as troops and equipment were seldom on the same ship, the two were often separated. This made for great confusion, which was only heightened by adopting the policy of giving one unit's equipment to another unit. Attempts to rectify the problem resulted in some units receiving two issues, and others none at all.[31] Some equipment was shipped broken down into components, a practice which virtually guaranteed that the equipment would not be reassembled at the destination. Mathematical calculations made by state-side logisticians proved inaccurate at D-Day and in some cases, the ETO never recovered. The smaller radios, the SCR-300 and SCR-536, suffered high mortality rates, yet replacement numbers from D-Day through the offensive were consistently too low.[32]

The problem still existed by December 1944. Naturally, the padding of equipment status reports, a trend which many argue continues today, ensured inaccurate supply and equipment allocations once the units had arrived in country and began to do their mission.[33] Ground and air forces competed for equipment, further complicating the problem. Although the amount of signal equipment shipped to Europe throughout the entire period of U.S. involvement in the war was less than two per cent of total tonnage transported, the importance of the equipment outweighed that lopsided ratio.[34] Communications equipment took on a degree of significance that far exceeded its bulk or weight, the standard logistics measures. Field wire was particularly critical;

although there was adequate wire in the theater to support the units in defensive posture along the Ardennes, once the attack had commenced and units had to quickly displace, much of the wire and cable could not be recovered.

Signal Security Equipment and Procedures

Although U.S. Army units at all levels used SOIs, higher echelon units had increasingly sophisticated equipment to secure their transmissions from enemy ears. Battalions used the M-209 encryption machine and the Slidex key. The SLIDEX was a radiotelephone code system by which mixed alphabets of letters and numbers were printed vertically and slid through a slot in a cardboard or metal holder. Operator personnel came with the M-209 but were critically short.[35] (See Appendix B, Figure 8 for a diagram of the M-209 machine). At division level, the SIGABA with appropriate operators was added, along with all of the previous equipment. This complement of equipment was echoed up to corps level. First Army also used the SIGABA and the M-209, but did not employ lower-level voice codes like the Slidex. One complaint from corps-sized units in particular was that the amount of code carried far exceeded that necessary, although they also complained that they did not have enough SIGABA machines.[36] U.S. forces also used the Playfair code down to regimental level, a British code first used in World War I. Invented by Charles Wheatstone in the 1850s, it was a quite effective system that had a rectangle of letters that were enciphered by digraphs, or two-letter groups. Thus the letters AZ and AL might encrypt into RD and GH, giving no indication that the first letter (A) in each digraph was the same.[37] This system was well-liked by the Americans, with V, VIII, XVIII Corps and the 99th Infantry Division reporting it as "very satisfactory" and "very effective" after the offensive.[38] (See Appendix C for a 12th Army Group Signal Security Questionnaire).

First Army Standard operating Procedures, and indeed, U.S. forces policy in general, required that most radio transmissions would be encoded. The American front line commanders

were issued Signal Operating Instruction books, which included brevity codes for more common words, and code names for units. The more conscientious commander would write out his message from the code book and give it to his radio operator to transmit, but because of the hasty transmissions required in combat, the books were sometimes not used. In fact, although Standard Operating Procedures and SOIs for virtually all units specified the use of codes and ciphers, it was an unwritten SOP that once in contact with the enemy, units should simply be brief and "cryptic" in radio communications.[39] Ease of use was the key to a good cryptographic system at lower echelons. It was bothersome for a staff officer at a large headquarters to wait for signal troops to encode and decode messages, but the few extra minutes an infantry platoon leader needed to encrypt his call for fire could differentiate between life and death.

Personnel and Training

Personnel and training shortfalls were a fact of war in the European Theater. Signal soldiers generally needed longer training times for the complicated equipment they were required to operate. Just as there was never enough wire, there were never enough wire construction troops to install it. There was also never enough maintenance personnel to take care of the radios and switchboards.[40]

With the added traffic due to the offensive, cryptographic technicians, particularly at corps, were in short supply. One division reported that although there were sufficient personnel on the TO&E, when casualties necessitated replacements they came to the unit relatively untrained. At both corps and division, there was a shortage of soldiers trained to operate and maintain the SIGABA and the M-209. At some points during the battle, as much as 90 per cent of traffic sent at army and corps level was highly classified and urgent, meaning that it had to be encrypted and sent quickly. Although the technicians initially deployed with the unit could handle the extra load, replacements did not have the training and experience necessary. Although

the Signal Corps requested and received special dispensation from the War Department to accept recruits only of the highest quality (see Chapter Three), after the offensive several units complained that their code clerks were not the "caliber of men needed for type of work that has to be done" and that the quality of replacements available was "far from satisfactory."[41]

The RI organization within FUSA (including the army RI company and the subordinate corps signal service companies) had undergone a significant training period in England prior to deployment to ETOUSA, but as an inspection by 12th Army Group's Signal Detachment "D" revealed in October 1944, there were still significant training and morale issues. With the exception of the First Army signal intelligence staff, which retained a British advisor, British trainers had just been released from the units, and the American soldiers were learning to operate on their own. Most units had leadership and training problems resulting from a lack of technical ability on the part of the senior non-commissioned officers. Inspectors rated high frequency interception across the board, as units did not choose their monitoring site well, nor did they periodically calibrate the radio sets which had the annoying tendency to "drift" off of the assigned frequency. Direction-finding activities, in particular, were rated as "most disappointing" due to both poor equipment and a lack of enemy signals upon which to practice. Moreover, corps level officers did not fully understand the theory of DF, nor did they ensure their troops understood the import of the intelligence they were intercepting. Traffic analysis, a matter of piecing together many details to make a coherent whole, was poor. Some units simply filed and then forgot messages, resulting in gaps in the enemy order of battle.

Telling comments wrapped up the report: to illustrate the good relationship between the signal intelligence organization and the G-2, the writer states, "As far as Intelligence itself is concerned, RI itself not always having a great deal to offer, has received maximum assistance" but that "at corps, the situation has been less satisfactory . . . corps G-2 have mainly had only

limited experience of the capabilities and requirements of RI."[42] This remark causes concern if one considers the following: in general, the lower-echelon RI elements were allowed to decipher low-grade artillery and maneuver unit traffic, and if deemed appropriate by the G-2, the information could sometimes be put to immediate tactical use as well as reported up the intelligence chain. However, the lowest level signal intelligence units were the corps-level signal service companies, so the corps G-2 was the controlling factor on the dissemination of intelligence.

The Offensive

Although some of the units involved were of questionable competence, signal radio intelligence and signal service companies at army and corps were constantly monitoring enemy tactical radio transmissions through radio intercept and direction finding.[43] This had been particularly effective against tactical units at division level and below throughout operations in the ETO. The radio silence imposed by Hitler in the weeks prior to the attack somewhat lessened the efficacy of this particular method for gathering intelligence, but many of the RI companies were reporting unusual activity in the weeks before the attack.

On 30 November, the First Army's assistant signal intelligence officer, First Lieutenant Bayard H. Hale, forwarded his monthly signal intelligence report stating that the morale of the newly formed 113th Signal Radio Intelligence Company was improving. Soldiers were keeping busy and had ample opportunity to practice their skills due to increased enemy radio activity. He referred to the increased enemy traffic again when he noted that the departure of British intercept service trainers gave him a chance to observe the U.S. soldiers operating on their own and performing well despite the unusually heavy load. The lieutenant also mentioned something very unusual in VIII Corps' 3245th Signal Service Company sector: the unit was still troubled with "dead air" or complete radio silence.[44] By then, of course, the Germans had moved the bulk of

their men and equipment forward, and were communicating by land line. Besides conspicuous changes in German radio traffic patterns, other possible tactical indicators of the offensive included a change-over from fixed to random call signs by the Germans in November 1944.[45]

In early October, the 12th Army Group's own 849th Signal Intelligence Service Company was reading messages that indicated the movement of armored divisions behind the Ardennes forest. Intercepts from subordinate RI units indicated the same. This information increased from day to day, but the G-2 took no notice.[46] Major R.E. Button at 12th Army Group was responsible for the preparation of the weekly Signal Intelligence Reviews, culled from the tactical intercepts of the Group and Army RI units, which he forwarded to the G-2. On October 26th, 1944, Major Button attached a handwritten note to his usual Signal Intelligence Review. It stated, "Note: The 'product' at 12th Army Group has been considerably greater than that of 21st Army Group for the same period."[47] There is a simple "very good" scrawled on the note to acknowledge its receipt. The bulk of German forces, of course, were building up opposite 12th Army Group's sector. In the report dated 6 December 1944, Button makes a similar statement, along with a bit of self-aggrandizement, "Throughout the period under review the Army and Corps (signal intelligence) sections have been especially productive for their G-2's. It needs to be emphasized, occasionally, that without the research and coordination effected at 12th Army Group, these units would be unable to function at all . . ."[48] After the offensive, however, Major Button stated in a memorandum to Sibert that there was "no indication" from the signals intelligence source that the enemy was planning an offensive for December.[49]

In defense of the intelligence community, it must be stated that German operational and tactical security was superb for this operation. Hitler had ordered that coordination for the operation would not be conducted over the wireless. On November 5, he also issued a directive which set forth a deception story: two reserve forces were to be established to counter a large

scale Allied offensive. To the north would be the larger of the forces, near Cologne, and to the south, near the Eifel, would be a much smaller force to contain the south flank of the envisioned enemy penetration.[50] Thus, some movements were allowed to take place in daylight in the north, to convince the Allies of a large force buildup, while to the south, the forces were better concealed and more carefully assembled. Ironically, the Americans assisted the Germans in their tactical security. Germans troops had been identified by American aerial surveillance in the past by sunlight glittering on exposed vehicle windshields and the smoke of cooking fires; intercepted American messages related these observations to the Germans. For the Ardennes offensive, however, German commanders carefully considered those lessons learned and took appropriate measures, including issuing near-smokeless anthracite coal for the soldiers to cook their meals.[51]

Vast amounts of troops and equipment, however, had to be moved to the Ardennes, and even though there was a robust wired infrastructure now that the Germans were back within *Festung* (Fortress) *Deutschland*, the wireless was sometimes used for expediency. Although it was true that ULTRA traffic slowed down as a result of Hitler's edict, it still remained a valuable source of intelligence in the weeks and days prior to the offensive. The Enigma machine's influence was felt not just in the military; federal agencies such as the *Reichsbahn,* the federal German railroad, used ULTRA for coordination, communicating with military units to plan transportation. In addition to the *Reichsbahn*-related traffic, requests for air protection of these movements encrypted both in ULTRA and lower level tactical codes became more common as the offensive drew near. Most requests for transportation and protection were concentrated on the Rhine crossings near Bonn and in the vicinity of the town of Koblenz. Both areas offered rail crossing by which trains might use the spur lines into the Eifel.[52]

The entire offensive was planned around a time when weather conditions would proscribe aerial surveillance, but Field Marshall Von Rundstedt also took advantage of the night,

sending vast amounts of equipment and manpower forward by rail during the hours of darkness.[53] His efforts, of course, were aided by the cavalier attitude of the Americans and their condescending air towards the "green" units on line in the Ardennes, disregarding the reports of noises and troop movements along the thinly held sector. Tactical signal intelligence indicators were also largely ignored. In addition, although ULTRA still offered a steady diet of intercepted messages regarding the buildup in the Ardennes, the intelligence officers at all echelons had been lulled into a false sense of security. At Third Army, General Patton's G-2, Colonel Koch declared on December 10 that a "spoiling or diversionary offensive"[54] was possible, but he weakened his assertions three days later to fall in line with the rest of his Intelligence brethren. Monk Dickson, too, had discussed the possibility of an offensive through the Ardennes with his SLU chief, Rosengarten, and as a result recommended to General Hodges that he ask General Bradley for two more divisions. Bradley replied he had none to spare.[55]

On December 10, Dickson issued a G-2 estimate warning of an offensive, but it placed the majority of enemy forces well north of the Ardennes. By the 15th he was already regretting his well-known impetuosity and issued another report that modified his earlier dire predictions to a "limited scale offensive." With that, he went on a four-day leave to Paris.[56] ULTRA had been so dependable in the past, clearly spelling out Hitler's intent and detailed plans, that anything less than a direct statement indicating an offensive was ignored.

Exploitation of German Communications

Although not appreciated prior to the offensive, the Americans enjoyed great success against the German radio systems despite the exhortations of enemy commanders and staff to encode all messages. This success is due to both intercept (which indicates poor encryption/code use) and DF. Although the Germans used very few lower grade codes prior to the offensive, increased Allied pressure had the effect of bringing low grade codes back to the air, allowing the

corps RI units to conduct more deciphering activities, and thus, get the intelligence out to the units more quickly.[57] During the offensive, enemy artillery units were the most productive targets, transmitting a wealth of easily deciphered messages in low-grade code. Artillery nets were easily identified, even when well encrypted, by the unique pattern of rapid interchanges between the forward observer, fire direction center and the firing battery.[58] They were closely followed by the loquacious tankers of the Panzer and Panzergrenadier divisions, especially the reconnaissance elements of the 130th Panzer Lehr regiment.[59] Thanks to radio intercept, the Americans knew ahead of time that the Germans were going to attack the defenders at Bastogne. This allowed the Third U.S. Army to attack the Germans on their flank, causing the attack to fail.[60] Prior to the offensive, 12th Army Group reports frequently cite intercepts from the Panzer Lehr Division and the 11th, 15th, 21st, and 116th Panzer Divisions. The 11th Panzer Division was a most cooperative player, although the traffic was "strangely resistant to cryptanalysis," but it was found after the offensive began that it was actually a fictitious unit and part of Hitler's ruse.

Logistics traffic also yielded much to the Americans, clearly indicating as early as the evening of December 16 that German units were already experiencing fuel shortages that in some cases forced them to proceed on foot. Tactical intercepts also indicated the enemy's intent to capture American fuel and food; in one case, a U.S. signal intelligence unit intercepted a message stating that the 130th Panzer Lehr Regiment had captured a number of U.S. vehicles. This capture was probably what allowed the 130th to advance relatively far. The difficulty of the German movement westward was further highlighted by a German captain's complaint that his movement was hampered by "the idiotic Military Police." [61]

Controlling Friendly Signal Security

The Americans were well aware that the Germans were eavesdropping on wireless conversations. Early in the offensive, ULTRA indicated that the insecurity of Allied communications allowed the Germans to form a substantially accurate picture of allied order of battle in the Ardennes Sector (see Appendix B).[62] Not only did Bletchley Park listen to embarrassing evidence of friendly transgressions over ULTRA, but the tactical RI units heard them as well, either directly from listening to friendly units or when addressed in German intercepts.. The issue was addressed obliquely in a memorandum from the FUSA signal intelligence officer, Lieutenant Colonel Summerfield, when replying to a request from now-Captain Hale of the 12th Army Group to extend the distribution of the FUSA Signal Intelligence Situation report to lateral armies. He recommended against distribution of the report as most of the information "is only of local interest and irrelevant to outside organizations,"[63] recommending that the reports be consolidated and sanitized at the corps level and that "anything which might reflect adversely on the units involved should be omitted."[64]

It is clear that the signal intelligence units were not focusing on friendly communications, and indeed, there were ample enemy targets, but what of the friendly monitoring which was to be accomplished by the SIAM units? Although SIAM units continually kept the army and corps under close supervision, there were simply not enough receivers and mobile teams to move forward, resulting in the front-line unit nets receiving "practically no service other than unit self monitoring."[65] A shortage of assets during the battle resulted in even corps units having no monitoring assets. Once the units were in the field, there were other problems. SIAM units did not have dedicated telegraph lines back to army headquarters and thus had to compete with other units to obtain wired communications to send their reports. As SIAM units were not considered a priority over other operational units and staff sections, they often had to resort to radio transmissions laboriously encrypted by a one-time pad.[66] First Army and Third Army report that

they used organic RI assets for monitoring friendly communications at subordinate units, and that they received special monitoring teams from 12th Army Group, but the V, VIII, and XVIII Corps and the 99th Infantry Division all reported that they were not monitored during the offensive.[67]

First Army's self-monitoring was largely aimed at the army headquarters. Organic RI assets conducted spot-checks of telephone lines and of radio nets. When security violations were found, the signal officer sent memorandums to the appropriate commander or staff officer. On October 1, the FUSA RI elements noted that V Corps units were passing important friendly intelligence unencrypted. These units revealed that the V Corps G-2 was authorizing these transmissions. Prior to the offensive, ordnance and signal units committed the preponderance of insecurities. After the Germans attacked, however, the artillery and military police nets displayed the most breaches of security as they coordinated fires and the movement of units forward.[68]

Jamming and Interference

Reports after the battle indicate the enemy attempted to break in to U.S. radio nets, and in some cases, succeeded. The XVIII Airborne Corps reported an enemy station entering the net with a captured radio. This was not corrected until callsign change-over, when the station failed to change.[69] This was not an isolated incident, as both armies captured enemy equipment and used in for their own purposes. German jamming was also a major problem throughout the offensive. The VIII Corps command net was jammed heavily, but the operators of the 149th Armored Signal Company with 9th Armored division were experienced and were able to copy through the jamming.[70] Less experienced operators, such as those in the 106th, were unable to communicate. This lack of communications was a major contributing factor to the 106th's disorganization, scattering of forces, and eventual capture.[71] In at least one instance, Germans used American radios from captured vehicles and effectively used them to jam artillery frequencies and to confuse American operators.[72] FUSA worked around the problem by routing

most traffic through the APOs with messengers, leaving the message centers free to concentrate on tactical traffic.[73]

On 29 December and continuing through 7 January, the Americans countered with the first and only battle test of the high powered airborne jammer, the Jackal. First Army had been reluctant to try the AN/ART-3 Jackal as a portion of the frequency band used by their tank radios overlapped into the jammed bandwidth. However, as the Jackal, like German tank radios, was AM, and the Americans were on FM, it seemed like a good opportunity to test it. According to German prisoners, the Jackal effectively knocked out German armor communications during a crucial period, and the Americans were not inconvenienced in the least.[74] Friendly interference, however, was reported to be a problem.[75] When units were jammed, they would switch frequencies in order to talk, sometimes jamming others inadvertently. In addition, attempts to operate through jamming sometimes caused enemy operators to revert to more easily understood plain text. The prevention of enemy communications was not only practiced over the airwaves, although the radio was the most lucrative target, particularly when, as in the Ardennes, the enemy was in the offensive. The Germans also used pigeons for communications, and when Americans came across enemy pigeon lofts or captured enemy pigeons, they clipped the birds' wings.

Conclusions

It is clear that, in general, the Americans practiced imperfect signal security prior to and during the offensive, although some units performed exceedingly well. Troops in combat did not always have the time to use unwieldy signal security devices or to follow complicated procedures. In addition, many of the American soldiers in the offensive were "green" and may have been poorly trained and inexperienced in signal security. As an aggregate, the intelligence community also performed rather poorly; not only missing key tactical indicators of the offensive available through signal intelligence, but by failing to always stress signal security. G-2

directives and an unwieldy structure to process signal intelligence resulted in tactical units not receiving timely information which may have been critical to their operations. The signal and intelligence organizations were aware of many of these problems and attempted to solve them. For instance, the signal intelligence officer at FUSA conducted daily radio intelligence meetings which encompassed both signal intelligence and signal security. FUSA put out many directives in the period before the offense, tightening up access to certain machines and codes, and encouraging strict adherence to codes and ciphers. FUSA also appeared to quickly and appropriately react to any security compromises.[76] Clearly, command, intelligence and signal structures recovered well from the initial shock of the offensive. Indeed, the very reason for American success in the Ardennes may have been the ability of the U.S. Army to quickly learn by its mistakes.

---

[1]George Raynor Thompson and Dixie R. Harris, The Signal Corps: The Outcome (Washington, DC: Office of the Chief of Military History, United States Army, 1966), 18.

[2]"First Army Combat Operations Data," 167.

[3] MacDonald, 61.

[4]Ibid., 53-54.

[5]Moe.

[6]MacDonald, 54.

[7]Ibid., 55.

[8] James L. Gilbert and John P. Finnegan, US Army Signals Intelligence in World War II. (Washington, DC: Center of Military History, United States Army, 1993), 189.

[9]Finnegan, 185.

[10]First U.S. Army Signal Service, Memorandum from Major Lawrence D. Summerfield, HQ, First US Army Signal Service, APO 230, dated 27 August 1944 to Signal Officer, HQ, 12th US Army Group, APO 655. Subject: Handling of Information derived from N/I Traffic, NA RG No 457.

[11]Finnegan, 211.

[12]Harley, 32.

[13]"First Army Combat Operations Data," 422.

[14]Ibid.

[15]United States, War Department. Table of Organization no. 11-77 Signal Radio Intelligence Company (Washington, DC: US Government Printing Office, 1942), 4.

[16]Henry L. Dull, Sr, "Post Mortem Writings on the Indications of the Ardennes Offensive, December 1944." (Carlisle Barracks, PA: U.S. Army War College, May 1977), NA RG No 457, 9,10.

[17]Thompson, Harris, 68.

[18]Report of Operations of 3325th Signal Information and Monitoring Company from 15 August 1944 to 1 July 1945, (APO 405, U.S. Army, 28 July 1945), Washington, DC: Records of the National Security Agency, NA RG No 457, 18.

[19]Ibid., 16.

[20]Woods, 232.

[21]Ibid., 235.

[22]Thompson and Harris, 92.

[23]Ibid., 157.

[24]Ibid.

[25]Moe.

[26]Raines, 277.

[27]Thompson and Harris, 119.

[28]Raines, 277

[29]Moe. Colonel Moe was the company commander of Company I, 3d Battalion, 423 Infantry Regiment, 106th Infantry Division during the Ardennes Offensive. He states during this interview that as the positions had been previously held by another division, the positions were well prepared and needed only minor improvements. The incoming 106th also inherited the wired communications equipment, which performed in an excellent manner in a large part due to the overheading of the wire.

[30]Woods, 234.

[31]United States Forces, European Theater General Board, "Signal," Study 110-112, Vol XXIV (Washington, DC: The War Office, 4 April, 1946).

[32] Thompson and Harris, 145.

[33]Ibid., 9.

[34]Ibid., 11.

[35]Twelfth U.S. Army Group Survey.

[36]Twelfth U.S. Army Group Survey.

[37]Kahn, 198.

[38]Twelfth U.S. Army Group Survey.

[39]Moe.

[40]Ibid.

[41]Twelfth U.S. Army Group Survey.

[42]First United States Army, Memorandum No. 4 on the SIGINT situation within First U.S. Army, dated 8 October 1944. NA RG No 457.

[43]Methods were virtually identical at both echelons, but the corps units tended to copy more voice traffic that did the army unit, although low volume voice traffic was not a particularly lucrative target. SRH-042, NA RG No 457, 7.

[44]First United States Army Signal Service, Memorandum from First Lieutenant Bayard H. Hale, Headquarters, First U.S. Army Signal Service dated 30 November 1944. Subject: Monthly Signal Intelligence Report. NA RG No 457.

[45]Memorandum, Hale, 30 November 1944, NA RG No 457.

[46]Kahn, 509.

[47]Twelfth United States Army Group, Memorandum from Major R.E. Button, G-2 Section, Headquarters, Twelfth Army Group dated 6 December 1944. Subject: Signal Intelligence Review, 21 November - 5 December 1944. NA RG No 457, 1.

[48]Ibid.

[49]Twelfth United States Army Group, Memorandum and note from Major R. E. Button, G-2 Section, Headquarters, Twelfth U.S. Army Group dated 31 December 1944 and 26 October 1944, respectively. Subject: Signal Intelligence Review, 15-25 December 1944. NA RG No 457.

[50] Dupuy, 106.

[51]Charles B. MacDonald, 48.

[52]Ibid., 65.

[53]Ibid.

[54]Ibid., 68.

[55]Ibid., 69.

[56]Ibid., 72-77.

[57]First United States Army, Memorandum from First Lieutenant Bayard H. Hale, Headquarters, First U.S. Army Signal Service dated 31 December 1944. Subject: Monthly Signal Intelligence Report. NA RG No 457.

[58]Stuart H. Schwark, Major, U.S. Army., interview by author, Fort Leavenworth, Kansas, 7 April 1997.

[59]Dull, 28.

[60]Third United States Army Signal Intelligence Service, SRH-042, "Third Army Radio Intelligence History in the Campaign of Western Europe." (Washington, DC: Records of the National Security Agency, NA RG No 457).

[61]Memorandum, Twelfth U.S. Army Group, 31 December 1944.

[62]Dull, 10.

[63]First United States Army Signal Service, Memorandum from Lieutenant Colonel Lawrence D. Summerfield, Headquarters, First U.S. Army Signal Service dated 13 December 1944. Subject: Signal Intelligence Situation Report. NA RG No 457.

[64]Ibid.

[65]Third Army Radio Intelligence History in the Campaign of Western Europe, 23.

[66]Report of Operations of 3325th Signal Information and Monitoring Company.

[67]Twelfth U.S. Army Group Survey.

[68]First United States Army, "Basic Records of First U.S. Army Signal Units: 29 May 1945." (Washington, DC: Office of the Chief Signal Officer, 29 August 1945). NA RG No 457.

[69]Twelfth U.S. Army Group Survey.

[70]Thompson and Harris, 161.

[71]Moe.

[72]Hugh M. Cole, The Ardennes: Battle of the Bulge (Washington, DC: Center of Military History, United States Army, 1993), 391.

[73]Thompson and Harris, 161.

[74]Ibid., 164.

[75]Cole, 654.

[76]First United States Army, "Basic Records of First U.S. Army Signal Units: 29 May 1945."

CHAPTER V

GERMAN SIGNAL SECURITY

Germany, like the Allies, made tremendous strides in communications technology during the period 1914 to 1918, the years of the Great War. In 1914, the Germans lagged behind other nations in their use of the wireless on the battlefield, and had no official agency to monitor enemy communications and glean intelligence. However, a chance interception of Russian signals during the battle of Tannenburg gave the Germans priceless intelligence on the intent of the Russian Second Army's commander, who had orders transmitted to subordinate corps in clear text in order to avoid any errors in encryption. As a result of some overzealous German newspaper reporters, the Russians soon realized what had happened, but by then the Germans had a taste of radio intercept and the valuable intelligence it could produce.[1]

As a result of that experience, the Germans began to concentrate on the art of intercepting wired and wireless communications, and then moved into the areas of goniometry and cryptanalysis. The Germans also practiced jamming in World War I, primarily against British air observers, although initial attempts were unsuccessful because the signals transmitted by the airplane radios were stronger than those of the jamming stations. However, this failure led to an eventual success. When the Germans switched their efforts from the aerial observers to interception of the British artillery calls for fire against German batteries, the latter were able to move before they could be destroyed.[2]

The British were not Germany's only targets on the Western Front during the Great War. The American Expeditionary Force is reported to have displayed "utter carelessness" with regard

to signal security.[3] Although the wireless had been regarded as the target of opportunity in the war against the Allied powers of France, Britain and Russia, it became of secondary importance against the Americans. The security of American telephones wires in the trenches was so abysmal that it readily yielded its secrets to the Germans, who employed the technique of earth telegraphy to intercept signals "leaking" through poorly insulated wire into the ground. The Americans gradually realized their security shortcomings and adopted codes and ciphers which placed them on an even footing with other nations already in the war.[4]

Germany's defeat in 1918 led to the Versailles Treaty imposition of a 100,000-man cap on the *Reichswehr,* the German National Defense Establishment, and a force structure consisting of seven infantry and three cavalry divisions. The cap resulted in an army allotment of seven signal battalions, each comprised of two companies, one of which included an intercept platoon. Signal personnel were also assigned to seven military districts, to the headquarters of the three cavalry divisions allowed under the force limitation and also to twelve permanent intercept stations positioned throughout Germany.[5]

Despite the harsh Treaty impositions, Germany's interest in the studies of signal intelligence and crytography did not wane. Although the Treaty did not provision for signal intelligence units other than the intercept platoons, the Germans had realized their value in the last conflict and had no intention of discontinuing research and development in the areas of signal security and radio intelligence. They carefully selected locations for permanent intercept stations and began to conduct radio intelligence operations.[6] The stations were assigned to guard specific foreign radio channels: British, French, Polish, Russian and Czechoslovak traffic were all observed, both diplomatic and military. Diplomatic radio traffic in particular provided valuable practice in cryptanalysis, and the Germans accentuated direction finding training to pin-point foreign military units on training maneuvers.[7] Besides the static radio intercept stations,

there were two other types of signal intelligence units: the divisions had short range interception platoons as authorized by the Versailles Treaty and there were a few radio intercept companies were attached to the army-level signal battalions.

In 1919 the army, in violation of the Versailles Treaty, established a highly clandestine twelve man intercept and cryptoanalytic service called the "Volunteer Evaluation Office." That organization was the genesis of the three military cryptographic services, one each for the high command of the army (*O.K.H.*, or *Oberkommando des Heeres*), the navy (*O.K.M.*, or *Oberkommando der Kriegsmarine*), and the air force (*O.K.L.*, or *Oberkommando der Luftwaffe*). These three agencies fell under the Chief, Armed Forces Signal Communications (*Chef, Wehrmachtnachtenrichtenverbindungen*, or *W.N.V.*) who served on the Wehrmacht general staff (*the O.K.W.*, or *Oberkommando der Wehrmacht*). The *W.N.V.* supervised all armed forces communications, including communications security and intercept operations, which was handled under the Cipher Office (the *Chiffrierabteilung*, usually abbreviated "*Chi*"). *Chi*'s duties included the supervision of international monitoring, development and control of ciphers, cipher supply, analytical cryptanalysis, practical cryptanalysis, interception of broadcast and press messages, and the evaluation and distribution of output.[8]

The Army Communications System (*Heeresnachtrichtenwesens*, or *H.N.W.*) was the oldest and most experienced military cryptographic and communications agency. Like the U.S. Army Signal Corps, it was responsible for both communications and intercept-cryptanalysis, and also like the Americans, it supplied its solutions to the army intelligence agencies for evaluation and use.[9]

Germany's decision to rearm in 1936 led to a force structure of twelve corps and thirty-six divisions with a proportionate number of General Headquarters (GHQ) units. The German military establishment was developing a great appreciation for the value of signal intelligence.

Emphasis from the top down was concerned with increasing the number of fixed and mobile intercept companies and intercept units were the first to be organized within the GHQ forces.[10] The mobile intercept units were initially assigned to army and divisional signal battalions. By late 1942, the German army attached short-range signal intelligence companies composed of the division's intelligence platoons to the army level signal regiments. These short-range signal intelligence companies included an evaluation team, a messenger section, one wire and one radio team for communications, a radio intercept platoon, three intercept/DF platoons, and a wire intercept platoon. The radio intercept and intercept/DF platoons each had thier own small evaluation teams as well.[11] General of the Signal Forces (*General der Nachrichtentruppen*) Albert Praun described the standard operating procedure for a short-range intercept platoon. He comments:

> Disregarding corps and division boundaries, the company usually stationed its evaluation center near a corps command post, together with the radio intercept platoon which was equipped with about thirty receivers but had no D/F teams. The principal mission of this platoon was to bridge the gap between long and short-range intercept operations. The three intercept-D/F platoons, which were equipped with fifteen receivers and three DF sets each, were moved as far forward as the situation permitted in order to be within effective ground wave range of the enemy field sets . . . however, each platoon had its own small evaluation unit staffed with cryptographers, who did not engage in cryptanalysis proper but decrypted messages with the help of complete sets of cryptanalytical solutions. Intercepts made by advance platoons were to be reported without delay directly to the staffs and units concerned, after which the data was reported to the intercept company headquarters.[12]

The company evaluation center would then compile all intercept information and send it to the signal intelligence battalion at army, which used virtually every transmission means possible, to include broadcast, to disseminate the information within the army area.[13] In contrast to the Americans, the army evaluation center would furnish the intercept companies with the solutions to commonly used enemy brevity codes and other cryptosystems to enable the lower-level evaluation teams to solve messages on a local level.[14]

In November of 1943, the Germans formed signal intelligence battalions out of the short-range and long-range signal companies, resulting in seventeen signal intelligence battalions and eight signal intelligence regiments, with an allocation of one regiment per army group. Based on further experience and tests on the Eastern front, the Germans further expanded the short range signal intelligence units by forming combat intelligence teams at division to replace the platoons that had been taken out to form the army short-range signal intelligence companies. They had also formed evaluation units at corps level to control these teams and to perform low-grade cryptanalysis.[15] This structure could quickly report, process and disseminate the results of intercepts and fixes. Some detractors advocated a plan to put the divisional teams back under the signal intelligence battalions, but tactical commanders quickly overrode them. The divisional commander zealously guarded his access to the relevant and quickly available information derived from signal intelligence.[16]

The Germans initially had difficulties in finding and training skilled operators. Like the Americans, who were unable to recruit "ham" radio operators because they were used on the home front, the Germans were also prohibited from recruiting them, as the Weimar Republic forbade amateur radio traffic in order to prevent subversive communications between the Communist Party and Soviet Russia.[17] However, the Germans' manning and training issues were addressed in the early days of mobilization by using a high percentage of permanent civil service workers, including women, for the fixed intercept units and reserving more trained males for the mobile units.[18] The training of linguists was an issue that required constant emphasis, particularly as the war expanded on different fronts and involved multinational enemy forces. The expanding signal intelligence force structure compounded the issue, as linguists operated not only at corps and army evaluation centers, but at the division as well, functioning to give the commander instant decryptions.[19]

By the spring of 1944, the Commander of the Staff of Signal Intelligence Regiment 5 in the German Western Theater Command (*OB/West*) had beneath him the regimental staff, three signal intelligence battalions, and the evaluation center consisting of 231 personnel. The duties of the evaluation center were to conduct the tactical and technical interpretation of all intercepted material independently of the fact that a quick evaluation had already been made at subordinate battalions. Decoding (the translation into clear text of enemy messages sent in known codes) and deciphering (the breaking of unknown enemy codes) were especially critical.[20] One battalion was attached to each subordinate army group. Signal Battalion 13 of Signal Intelligence Regiment 5 was employed in the zone of the Army Group B, with its staff in the region of Lille. Signal Battalion 13 was composed of three companies, the 2d and 9th Signal RI Companies (fixed) and the 613th Long Range Signal RI Company (Mobile).[21]

The Germans had learned through experience in the East and in Africa that a centralized structure was much more efficient, and thus army group and army headquarters had no authority or control over the signal intelligence battalions.[22] German security regulations, however, did not prohibit unit commanders at virtually any level from using an extra radio receiver to attempt their own intercept work and use the results as they saw best. Germans also used these radios to break in on Allied nets and either jam them or to give false orders, sometimes to great effect. Neither practice was discouraged by the German intelligence or signal communities, nor was it regulated in any way.[23]

The employment of signal intelligence units in the West was primarily dependent upon enemy concentrations and by the capabilities of the unit. The long-range company intercepted strategic-level traffic, while the other units collected operational and tactical intelligence that had immediate use to a maneuver commander. Monitoring the Allied buildup to establish the center of troop concentrations and movement in Great Britain became the main mission of the long-

range reconnaissance companies in the West. After the Normandy invasion, the long-range units continued to monitor the British Isles and then shifted their focus to monitoring Allied traffic along the French coast. Short-range units, on the other hand, concentrated on units in contact with German forces, focusing mainly on the lucrative targets of the artillery and armored unit nets.[24]

In the interests of speed, the Germans decoded tactical messages at the lowest possible level. They had learned in the East the tremendous value of low-level signal intelligence, although all interceptions were passed to higher echelons as well. If an urgent clear-text message was intercepted, the division's signal intelligence team immediately provided the information to its G-2 and corps evaluation unit simultaneously. Like their American counterparts, German signal officers developed close working relationships with their G-2s, but in general, the Germans considered signal intelligence as primarily a responsibility of the signal officer, who directed the employment of all signal intelligence units and who was the focal point for all signal intelligence reports,[25] although the G-2s might receive simultaneous reports. Messages intercepted by the long- or short-range companies were sent to their battalion's evaluation center for decoding, and were further sent up to the regimental evaluation center if it could still not be solved. Unlike some American RI units, German signal intelligence units enjoyed priority use on teletype circuits to the army and corps headquarters.[26]

To quickly disseminate critical information, a broadcast transmitter at evaluation centers was used; every army group, army, corps and division had a radio specifically for the purpose of receiving these transmissions. If units sometimes received messages for which they had no concern, this disadvantage was outweighed by the many lives saved through timely warning.[27] Notification usually occurred within two hours of intercept, and the information often included Allied bombing and artillery targets, Allied troop movements and locations near German units,

and any report revealing knowledge of German maneuver plans and unit locations. Rapid movements of the enemy did not greatly confuse the German signal intelligence units, as they practiced an extremely effective method of sharing traffic evaluation data on enemy units.[28]

The structure under which German army RI units fell for the Ardennes Offensive was in part due to the wrath of *Luftwaffe* commander Field Marshall von Richthofen over an incident during the Italian campaign. A German RI unit sent an intercepted message revealing a planned Allied landing to German army units in the theater and to the intelligence officer of the *Luftwaffe.* The intelligence officer delayed giving it to Richthofen until a planned staff meeting. As a result, the L*uftwaffe* was unable to counterattack in time and the landing was successful. The Field Marshall was furious, demanding that such reports would be sent directly to him or his chief of staff, and simultaneously to the units concerned.[29] The Germans used this very successful practice of simultaneous dissemination until the end of the war.[30]

Communications Equipment

During the First World War, nations developed communications equipment more or less along parallel lines. However, the Germans quickly rose to the forefront of wired communications technology for World War II. At lower echelons, Germans used the small, lightweight switchboards that were so popular with the Americans. At division and higher, there were great improvements to wired communications. Four-wire field trunk cable had been developed before the war, permitting several telephone and telegraph messages to pass simultaneously over a longer distance than was capable before. Later in the war, up to forty simultaneous circuits, either telephone or telegraph, could be run over two bare wires on one carrier frequency. Switchboards and telegraph adjuncts were developed to support this technology. It was vastly superior to the Americans' technique which needed separate wires for

every circuit.[31] When Allied air raids on the Western Front hampered communications, General Praun commented:

> The situation led to the decision to transfer the continuous transposed open-wire system, which with the aid of carrier frequency equipment could be used for multiple channel communication and had proved so successful in the East, to behind the new fronts in order to supplement the trunk-wire network. In the few months before the end of the war the operation signal regiments erected about 15,000 kilometers of continuous transposed open-wire systems between north and south, and east and west, a valuable new network which was almost entirely enclosed in the interior of the Reich and worked splendidly up to the last days of the war. In this way it was possible to construct the most important communication systems of the supreme army command on a priority basis with comparatively little material.[32]

Germany taught the Allies a valuable lesson in the beginning of the war through the coordinated use of armor and close air support backed by motorized artillery and infantry. The key to this mobility was effective communications as effected by the radio.[33] Although German field troops did not make the change to the more efficient FM radio, they made good use of some of the higher frequencies for inter-tank communications. The German army's success with mobile radio led General Praun to comment:

> Of particular importance was reliable radio communications between tanks and motorized units, and this applied not only to the troops in combat but also to communications between the staffs of the armored corps, armored and motorized divisions, and their regiments. As shown by successes in many different campaigns this problem of communications between tanks was solved admirably by means of ultra short-wave equipment . . . Command was most flexible where the classic Guderian in France and Russia, Rommel in France and Africa, hurried from one point of main effort to another accompanied by their "general sections" (Generalstaffel), which were later imitated by many other commanders, and an armored radio section with a few tank operators, to command their armored divisions, armored corps and armored armies exclusively by radio from the foremost line.[34]

Prior to the U.S. involvement in the war, the German army was already equipped with radios down to the company level, while the U.S. Army Signal Corps was struggling to develop an adequate radio design for tactical troops.[35] By the time of the offensive, however, the German army was suffering from a lack of materiel in general, to include radios, although the divisions in the offensive varied greatly in terms of the quality of their personnel and equipment. The

volksgrenadier divisions were in the worst condition, with inexperienced officers and men, and insufficient equipment.[36] The Germans, however, considered that the Americans had too many radios, which contributed to SIGSEC violations, and were themselves not significantly hampered by radio shortages.

Cryptographic Equipment

Evidence leads us to believe that the Germans were quite aware that their transmissions were being intercepted.[37] A German POW captured at the Anzio bridgehead on 31 January 1944 gave the following statement, "There were several indications of allied interception notably the accurate artillery fire which would often follow up within a few minutes of a wireless call."[38] Thus the Germans were quite diligent in thier signal security efforts. The German army established three categories for its cryptosystems and used the same standards to classify enemy systems: higher ecehlon traffic demanded "absolute security within the limits of feasibility,"[39] intermediate-echelon traffic security needed to be effective for about three days, and for combat messages, a few hours was sufficient.[40] Perhaps because of this classification system, they employed a less varied list of cryptological equipment than did the Americans. For instance, the glowlamp Enigma machine was used for high-level communications from *OKH* to regiment. A proven performer, it functioned equally well in the Russian winters as the Libyan summers. Thought secure if the key were changed thrice daily (as directed in 1942), the Enigma was battery operated and portable and could be operated in a moving truck. It was well adapted for radio work. Its only disadvantage was that it could not print its output and required three men to operate - one to read the encrypted character off the message and strike the correct key, one to read the decrypted character that showed up in the window, and another to write it down.[41]

For wire teletype transmissions from the *OKH* to army corps and a few divisions, the Germans used an on-line machine manufactured by Siemens and Halske Aktiengesellschaft based

on a keywheel system. Teletypes would transmit in characters composed of five pulses, the permutations which would form letters, numbers and punctuation marks. The Siemens machine would encrypt or decrypt these pulses, and either transmitted or printed them in a single operation.[42]

For non-machine applications at regiment, battalion and company, the German army used the double transposition, or columnar method. This was a tedious process of at least six steps involving a paper code. Each division produced these codes, printing at least three for its subordinate units. For intelligence and combat reports, a code word system was used, comprised of two and three-character alphanumeric codes which were also produced at division. As the troops "heartily disliked" the columnar method, they sometimes substituted the code or more frequently, sent the message in clear text. This led to great frustration on the part of many signal officers, and eventually the columnar method was scrapped and replaced by a modification of the grille.[43] The grille was a sort of template with windows cut in it which the writer placed over a sheet of paper. He wrote out the message in the holes, one letter per hole, in a normal writing style of moving from left to right across the page. He then lifted the template, or grille, and filled in the letters around those already written so that an innocuous message emerged. Some very odd-sounding messages resulted.[44] In addition, lower echelon forces used special ciphers such as the Playfair code for the encryption call-signs, numbers and other specific information.

Actions Against the Americans

Signal Intelligence Regiment 5's Signal Battalion 13 was employed in the zone of the Army Group B, with its staff in the region of Lille. American maneuvers and then mobilization was followed carefully by long-range German RI units listening to skywave from the United States. The interceptors would follow the American clear-text messages which assigned units to APOs to trace the units' movements from stateside to Britain, and then to Europe or North Africa.

The Germans also exploited promotion messages for the same purpose, having established personnel files culled from stateside maneuver intercepts.[45] When the Americans entered combat, the short range RI units were able to intercept their communications, and although the higher grade SIGABA remained undecipherable, the Germans were able to break many field codes. For instance, at first it took the Germans up to four days to decrypt an M-209 transmission, but after the device was compromised in North Africa in 1942,[46] they only needed a few hours.[47] Even so, the Germans typically did not concentrate on mechanically encrypted messages; there was a wealth of tactical information to be gleaned from the Allies that required far less work and could be used much more quickly. As early as mid-January, for instance, the Germans knew from low-grade intercepts that the Americans were not interested in creating another Falaise or Mons Pocket in which to capture the German forces. As the Battle of the Bulge drew to its end, these messages proved to be correct, and the Germans were able to pull the panzer divisions successfully out of combat, with only a minimum of rear-guard fighting. Interestingly enough, the Americans had intercepted German messages referring to this piece of signal intelligence, a point that highlights the fact that the Americans should have been well-aware of enemy intercept operations.[48]

Information obtained from captured intercept records and an interview in 1944 with the Alsatian Wachtmeister confirmed that clear text and place names were an extremely important source of intelligence to the Germans. In fact, the Wachtmeister stated that if a German intercept team encountered code on a frequency they would immediately change the frequency to another to find clear text instead.[49] General Marshall Fritz Kraemer, Chief of Staff of the I SS Panzer Corps and later Chief of Staff of the 6th Panzer Army, said flatly of U.S. forces:

> Radio discipline was bad. During the retreat to the west and more particularly in the course of the Ardennes offensive, we intercepted countless radio messages, some of which were in clear. The names of localities were rarely or never encoded, so it did not always require much effort to grasp the meaning of a radio message.[50]

Intercepted ULTRA messages confirm this. Those interceptions and the 1944 interview with the *Wachtmeister* prompted the allies to make the following statement:

> The decentralization of the German intercept organization to Div HQ evidently presents the large amount of technical liaison between sections that is necessary to identify networks. Its "dividends" seem likely to disappear if we institute the use of map reference codes that MUST BE used in conjunction with clear text messages. The fact that these small parties of "interpreters" drop any cipher or code traffic, seems to indicate that a Map reference code of low security but really EASY to use quickly and so acceptable to forward troops in operations would cause them great difficulty and confusion if they tried to tackle them.[51]

Allied call signs were often the same for a unit over long periods and even frequencies remained unchanged for weeks at a time.[52] The effect of fixed call signs and poor procedures was confirmed by ULTRA intercepts during the buildup: "ULTRA clearly indicates that insecurity of Allied communications allowed the Germans to form a substantially accurate picture of Allied Order of Battle in the sector south of Aachen."[53]

Situation reports gave not only their dispositions and often gave the names of particular officers in the unit, but also let the Germans know that the Americans often knew the enemy disposition very clearly as well. This was evident particularly on artillery nets during calls for fire upon enemy positions. Hugh Cole, the official U.S. Army historian of the Battle of the Bulge, wrote concerning the American defense of the town of Krinkelt: "Communications between the firing batteries on Elsenborn ridge and the rifle companies in buildings and foxholes functioned when needed - although the losses suffered among the artillery forward observers were unusually high."[54] This tactical intelligence, when processed swiftly enough, enabled the Germans to quickly move forces, sometimes avoiding fire, and even allowed them to counterfire upon the Allies.[55] It also allowed the Germans to improve upon their field discipline; intercepted reports revealing that the Americans could see the German troops because of poor cover and

concealment such as the glitter of exposed vehicle windshields led to the superb tactical security practiced by the Germans during the buildup in the Ardennes.[56]

The Americans were vulnerable in other ways than clear text transmissions. The Germans had been reading M-209 messages for at least two years and the Slidex code had been broken by the German intercept of maneuver traffic in March of 1944.[57] Captured American crytpographic material allowed the enemy access to U.S. communications as well, but fortunately, the Germans frequently announced the capture of such material. For instance, on 23 December, the 130th Panzer Lehr Division sent out word that it had captured an SOI belonging to the 10th Armored Division. An American 12th Army Group signal intelligence unit intercepted this report, and the Americans were able to change to an alternate SOI, canceling the compromise.[58]

As did the Americans, the Germans rated their enemy in terms of signal security. In general terms, artillery and armored forces were the easiest for the Germans to target, if not by the use of clear text, call signs or place names, then by the nature of their transmissions. Of the Allied forces, the British exercised the most stringent signal security and the French, the worst.[59] The Americans fell somewhere behind the British; of the American forces, the U.S. Seventh Army offering the greatest challenge to German cryptographers because of its exceptional radio discipline and cryptographic security.[60] The Germans rated Patton's Third Army as the easiest to observe among American forces; then-Lieutenant Colonel Creighton W. Abrams, battalion commander of the 37th Tank Battalion of the Third Army, was famous for bothering with neither call sign nor code. "This is Abe," he would say over his tank radio.[61] As well as engaging in careless message transmission, elements of the Third Army transmitted their new passwords twenty-four hours in advance, giving the Germans ample time to decipher them before they were to become effective.[62]

As stated earlier, through radio intercept, the Germans were able to determine the American's plans and order of battle prior to the Ardennes offensive to include the composition of units, weakly held sectors, and the lack of reserves. Even as the Germans advanced, they were able to track U.S. withdrawals and reports of heavy casualties, as well as information about their own forces.[63] A few days after the initial attack, German intercept units picked up a new net: American Military Police were reporting all major troop movements - including advance guards, march velocities, and column lengths - in an easily broken cipher abundantly interspersed with clear text. The Germans were also able to discern with which divisions Patton's army was going to strike, the concentration of Americans at the Remagen bridgehead, and the direction of intended armor thrusts.[64]

German Signal Security

It is evident that the Germans clearly understood the value of tactical radio interception, part of what they termed the "passive" radio services: receiving, direction finding and cryptanalysis. The "active" services consisted of technical improvements in communications and cryptological equipment, by speed and accuracy in operation, by changing procedure and by careful transmission - in short, what the Allies termed "signal security."

The Germans issued again and again stringent instructions with regard to signal wireless scrutiny. Great emphasis was laid on the necessity for codes, and the avoidance of plain language. German officers cautioned SIGSEC by relating that Russians had allegedly been condemned to death for non-observance of the rules prohibiting passing messages in the clear.[65] The veracity of this statement is further evinced by the wording of German documents enforcing SIGSEC. Just as the Germans identified armor and artillery as the primary Allied violators of SIGSEC, so did they accuse their own:

> It is authenticated that the enemy intercept service has obtained time after time valuable results from observation of our W/T activity. It must be accepted that, daily, well trained German tank men must lose their lives and innumerable tanks must be destroyed because particulars of strengths, organization, and locations, attack objectives and supply states have become known to the enemy as a result of careless R/T traffic.[66]

Another directive stated succinctly, "All W/T traffic is capable of being intercepted by the enemy. All W/T messages are capable of being intercepted by the enemy. There is absolutely no safe cipher."[67] Despite these dire warnings, however, a written authorization from the tactical commanders would still permit operating procedures to be relaxed in cases of extreme urgency.

The Germans were quick to realize the importance of both signal security and signal intelligence. Their attempts to deny signal intelligence to the enemy generally paralleled that of the Allies; although the Enigma had been compromised quite early in the war, the machine itself was strikingly similar to the American SIGABA. Germans soldiers used Playfair codes and one-time pads, much as the Americans did, and like the Americans, blundered by occasionally transmitting in clear text or not encrypting names or locations. More so than the Americans, the Germans generally regarded signal intelligence as a very reliable form of intelligence, one which could, more than any other intelligence source, give the commander immediate tactical advantage. Thus the Germans tended to concentrate on lower level nets, and then further examine those which were plain text or easily enciphered.[68] While this may at first appear to be laziness on the part of the operator or his immediate leadership, it in fact reflected the Germans' doctrine of rapid decode to ensure rapid dissemination, which in turn would allow tactical commanders to act quickly while they had the advantage of recently acquired intelligence. Because of this concentration on field material, the Germans had no significant strategic or operational success as the Allies did with ULTRA.[69]

Field Marshall Kesselring, the intelligence officer at Army Group West, estimated that 95 per cent of the Germans' intelligence for the Ardennes Offensive came from signal

intelligence. Air reconnaissance was impossible due to the deception plan and Allied air superiority, few POWs were captured, and spies could not get behind the front. Yet because of Germany's weakened condition and the American superiority in terms of manpower and materiel, it was unable to exploit that intelligence.[70]

---

[1]Praun, 151.

[2]Ibid., 153.

[3]Ibid.

[4]Ibid., 154.

[5]Ibid., 155.

[6]Ibid., 155-156.

[7]Ibid., 158.

[8]Kahn, 454-458.

[9]Ibid.

[10] Praun, 161.

[11]Ibid., 173-174.

[12]Ibid., 174.

[13]Ibid., 175.

[14]Ibid., 193.

[15]Ibid., 161.

[16]Ibid., 173.

[17]Ibid., 195.

[18]Ibid., 163.

[19]Ibid., 165.

[20]United States War Department, "A Study of German Operational Intelligence," (Washington, DC: Chief of Military History, 1946), 11-13.

[21]Praun, 72.

[22]"German Operational Intelligence", 8-10

[23]Ibid.

[24]Praun, 67.

[25]Ibid., 28.

[26]Ibid., 13.

[27]"German Operational Intelligence", 12-13.

[28]Praun, 75.

[29]Ibid., 65.

[30]Ibid., 66.

[31]Woods, 203.

[32]Ibid., 204.

[33]Ibid., 231.

[34] Ibid., 232.

[35]Woods, 200.

[36]Dupuy, 47.

[37]"Safeguarding the Radio Traffic of Signal Units of the 3d Reich, 1944," SRH 387, NA RG 457, 2 (hereafter referred to as SRH 387).

[38]Ibid.

[39]Praun, 228.

[40]Ibid.

[41]Kahn, 459.

[42]Ibid.

[43]Ibid. For a good explanation of how a transpositional, or columnar code works, see Kahn's The Codebreakers, page 301.

[44]Ibid., 144.

[45]Praun, 48.

[46]Kahn, 460. The solution of M-209 messages in North Africa gave such tidbits as the fact that American forces were prevented from shooting at any airplanes (as they may possibly be Allied planes).

[47]Ibid., 77.

[48]"Third Army Radio Intelligence History in the Campaign of Western Europe."

[49]National Archives, "Critical Examination of German Intercept in world War II," (Washington, DC: Records of the National Security Agency, NA RG No 457.)

[50]Fritz Kraemer, "I SS Panzer Corps in the West in 1944," Military Study No C-048, (U. S. Army European Command, Historical Division), 35.

[51]"Critical Examination of German Intercept."

[52]"German Operational Intelligence," 8.

[53]Dull, 10.

[54]The Ardennes: Battle of the Bulge, 124.

[55]"Critical Examination of German Intercept."

[56]Praun, 63.

[57]Thompson and Harris, 91.

[58]Memorandum, Major R.E. Button, NA RG 457, 2.

[59]Praun, 69-72.

[60]Ibid., 81.

[61]Lewis Sorley, Thunderbolt (New York: Simon and Schuster, 1992), 55.

[62]Praun, 82.

[63]Ibid., 84.

[64]Ibid., 86.

[65]SRH 387, 2.

[66]Ibid., 3.

[67]Ibid.

[68]"German Operational Intelligence," 27.

[69]Ibid., 27.

[70]Praun, 86.

CHAPTER VI

ANALYSIS AND CONCLUSIONS

Neither the German nor the American armies exercised tactical signal security in an exemplary manner prior to or during the Ardennes Offensive. Although the Germans enjoyed considerable success in their early deception plan, this resulted more from to the Allies' dependence on ULTRA than to the Germans' excellent signal security. In Hitler's Last Gamble, Trevor Dupuy writes, "The Allies' reliance on ULTRA had infected the high-command intelligence staffs . . . with a pervading sense of complacency. The older means of intelligence gathering were not only less depended upon but considered to be less dependable."[1] Clearly, the importance of tactical signal security was overlooked by the Allies and that error was a major contributing factor to the ability of the Germans to create such a large salient into American lines. There is more to the story, however, of signal security and signal intelligence in the Ardennes offensive than the initial deception plan.

German and American forces in the Ardennes used similar communications systems and cryptographic systems of comparable technological value. German wired telephone technology was generally equal to, and in some respects superior to, similar American technology. In fact, Americans preferred the light-weight German tactical switchboards over their own cumbersome pieces. Germans lacked FM technology, but had superior experience in mobile radio communications, particularly infantry-tank communications. German cryptographic equipment and material was very similar to that of the Americans. The German Enigma was functionally much like the American SIGABA, although the Germans used their machine down to regimental

level, and Americans did not employ the SIGABA below division. Both armies used code words, one-time pads, and Playfair codes.

Signal interceptors in the U.S. Army found German reconnaissance elements to be quite helpful in revealing the intent of German units. Armor and artillery units on both sides were rated by the other army as having the worst signal security. Both German and American soldiers hated unwieldy codes and found excuses not to use them. All units, regardless of nationality, exercised better signal security in the defense than in the offense, when the risk of unsecured transmissions was judged to be less than the risks associated with staying too long in one location and drawing enemy fire.

Although the Germans rated British communications as the most secure of all their opponents, the Americans were quite respected; U.S. radio operators were deemed fast and sometime very experienced, but as soon as the U.S. forces entered combat, radio discipline degraded rapidly.[2] The Germans discovered vast differences between the signal security of different armies, and went so far as to say that there appeared to be no centralized radio command agency charged with imposing uniform standards for signal security.[3] In the Ardennes offensive, the Germans credited the Military Police with violating all established rules of signal security, giving the Germans "complete information on U.S. plans and operations."[4]

Both armies suffered from equipment shortages in the Ardennes. The American theater reserve turned out to be inadequate, and the equipment on hand could only be released by the theater or COMMZ signal officer. The problems associated with equipment -- getting the right equipment in the right quantity to the right unit in an operational state -- originated with D-Day and were never truly solved. Units had a particularly difficult time obtaining communications wire and repair parts. American units surveyed after the offensive indicated that they needed more communications and cryptographic equipment. The XVIII Corps stated they could have

used two more SIGABA machines as they had taken only one with the forward echelon. Third Army also related that the six required SIGABA machines were not enough: "When 90 per cent of the traffic is OP and URGENT, it is impossible to clear all messages in time limit allowed for this type traffic."[5]

Interestingly enough, although the Americans generally criticized the lack of communications and cryptological equipment, compared to the Germans, they were over-equipped. The Germans attributed the over-abundance of U.S. Army radios at the tactical level providing many clues regarding the tactical situation and U.S. intentions.[6] The American forces exercised poor signal security while moving into their positions in the Ardennes; as a result, the Germans had near-complete information on U.S plans and disposition of units.[7]

By the time of the offensive, Germany was laboring under a severe lack of raw material which significantly slowed military equipment production. Because of overall equipment shortages in the German army, many of the German units in the offensive were short combat equipment.[8] As German doctrine, however, was built upon mobile communications, and the entire German offensive plan was built upon swift strike and rapid maneuver, Germans units in the offensive did not suffer from a lack of radios.

Both armies employed radio frequency changes as a signal security measure, although the Americans, with their larger complement of radios competing for frequencies, were less successful than the Germans. The Americans not only had a large contingent of support units with radios, but also had to contend with Allied radios, an issue which greatly complicated frequency management. Tactical commanders and their radio operators did not want to cooperate in solving the problem. David L. Woods, in A History of Tactical Communications Techniques, observed:

> The main difficulties (with radio communications) were the congestion of the frequency spectrum and the complications arising from security precautions. Not the least among the

> latter was the reluctance of commanders to frequency allotment changes being made during the course of operations as often as security considerations demanded.[9]

In addition, the unnecessary retention of frequencies by units in the rear led to the reuse of frequencies in front-line units. Both the abundance of radios and the reuse of frequencies assisted the Germans in targeting and intercepting American radio traffic. This advantage was offset after the offensive began, however, as the Germans left their wired positions and had to rely solely on the radio for communications. The Germans then became the most vulnerable to intercept.

Although a lack of frequencies might have been partially responsible for American failures to change frequencies as often as required, inadequate training and discipline in both armies were also major factors contributing to poor signal security. Many of the American units in the Ardennes, though fully manned and equipped, were new to combat and perhaps inadequately trained in signal security. Certainly, the shock of the initial offensive caused many U.S. soldiers to disregard security precautions in their rush to communicate.

The Germans also had to contend with a lack of training. Their problems were not just due to inexperienced troops, but with the lowest quality of soldiers seen in the German army to date during the war. Most of the German army stayed on the Eastern Front, even after D-Day, including the majority of German first-rate units.[10] Although most units had experienced officers, many of the *Volksgrenadier* units had been filled with retrained *Luftwaffe* or navy men who had seen little ground combat. Even the elite *SS* divisions were in relatively poor shape. Although they were technically overstrength in personnel, much of that manpower consisted of ethnic Germans from conquered countries and more navy and *Luftwaffe* men.[11] Combat experience had a direct correlation to signal security: experienced troops not only understood the calamitous effects of poor signal security, but over time, developed the ability to judge when the urgency of a situation demanded a fast transmission in clear text, or if they could afford to take

the extra time needed to send out an encoded message. Even the most experienced officers simply could not be in all places at once; consequently, they cannot constantly ensure that all members of their units are practicing good signal security.

Although there were many references to poorly trained and undermanned German combat units, most documents indicate that the German RI units were well trained, fully manned and adequately equipped. German intercept units at all echelons had been more or less in continual service since the early 1920's. Although the Germans suffered some of the same hardships as the Americans in finding adequate personnel during the increased mobilization period prior to World War II, the Germans had a highly evolved signal intelligence structure with a full complement of well trained and experienced officers and non-commissioned officers to train new inductees.

As the Germans honed the skills and organization of their RI units, the American army, who had allowed wireless technology to pass it by in the 1920s and early 1930s, was struggling to simply field adequate tactical communications for its burgeoning ground combat units. Naturally, the U.S. Army Signal Corps needed to concentrate on producing friendly communications assets before targeting those of the enemy for exploitation, and as a result, did not start manning and training signal intelligence units until relatively late.[12] In addition to overcoming its slow embrace of technology, the Signal Corps had to may still have had to contend with the legacy of Henry Stimson and his admonishment that "Gentlemen do not read each other's mail."[13] Additionally, most U.S. Army intercept units have the benefit of experience in long-range intercept, as did their enemy. While the Germans needed only to shift their focus from fixed, long range intercept, DF, and decryption to operations at a more tactical level, the Americans had to start from an experience base of little more than approximately three hundred SIS soldiers and civilians.[14]

Although the U.S. Army signal intelligence structure grew rapidly, many signal intelligence units were not formed in time to allow for extensive training before deploying to the ETO. According to external inspection results from 12th Army Group and internal assessments, First Army's signal intelligence units were poorly trained upon their arrival in Europe. Despite the efforts of the British trainers sent to assist them by 12th Army Group's Signal Detachment "D," in late October of 1944, less than two months before the offensive, FUSA RI units were still performing their duties in a substandard manner.[15] Despite problems in training, experience and morale, however, they still managed to target, intercept and decode a significant quantity of German communications.

Other manning and training issues throughout the signal community no doubt affected American signal security as well. A 12th Army Group after action survey indicated that a lack of trained personnel on the SIGABA machine caused operational difficulties at both army and corps level. At all levels, units recommended that the enlisted men working on cryptographic systems have higher ratings and simply should be of higher caliber. VIII Corps reported both the rating and the quality of the men assigned as "far from satisfactory" and further recommended that the men be trained in the service battalions before being assigned to the unit, implying that on-the-job-training was a common occurrence.[16] In addition, Third Army stated after the offensive that there were no communications maintenance personnel at Third Army Headquarters.[17]

Notwithstanding the many similarities between German and American signal security and signal intelligence training and equipment, one tremendous disparity remains. While American leaders were encouraged by their intelligence structure to ignore tactical signal intelligence indicators, German commanders very clearly realized its import. In the German army, tactical commanders, from division level up to the chief of the Army General Staff, attached paramount importance to signal intelligence and used it extensively in formulating their decisions.[18] The

German army, then, built a signal intelligence structure that could unrestrictedly provide the tactical commander with immediate intelligence. The signal regimental commander ensured that his RI units at the lowest level were supplied with up-to-the-minute enemy ciphers to allow them the maximum flexibility in quickly deciphering enemy messages.

The German concept of "centralized control, decentralized execution" presents a marked contrast to the U.S. Army, which allowed corps signal service company units to decrypt low-level code only. Certainly, timeliness of decrypt and the dissemination of the resulting product back to the field commander suffered as a result of that policy. The Germans, however, were able to quickly pass the intelligence they obtained to tactical commanders through a highly effective broadcast system, without having to pass it through a filter of intelligence officers (who may or may not have deemed it appropriate for dissemination). In fact, as related by General Albert Praun, German intelligence officers played a very small part in signal intelligence or signal security:

> German cryptanalysis was always directed by highly competent signal officers with experience in radio communications and intelligence, and in tactical and technical problems involving signal functions. To place this organization in the hands of cryptanalytic experts would not have been practical, because, however qualified they were in their own spheres, they lacked the necessary perspective and understanding of the techniques of the enemy's radio communication.[19]

In contrast, although American signal security was mostly a Signal Corps function, U.S. Army intelligence officers primarily directed the activities of American RI units. It was acknowledged among intelligence officers themselves that the U.S. Army intelligence community enjoyed a less than favorable reputation. While such a reputation may have been undeserved, American intelligence officers of the 1940s were certainly products of an army, that in comparison with the German army, had lagged significantly behind in terms of the development and appreciation of signal intelligence, and were themselves untrained in the employment and

benefits of such. The very success of the initial German deception plan demonstrates the validity of this statement.

Another difference between the two armies would appear to be the existence of the American SIAM companies, indicating a strong U.S. Army concern over signal security, although the concept was actually copied from the British. Those SIAM units, however, ended up actually doing very little monitoring and focused instead on the status of friendly troops. A 12th Army Group survey after the battle indicated that only the First and Third Armies used SIAM monitoring to ensure signal security compliance.[20] Corps and division units stated that they did not have any monitoring assets. In actuality, units employed self-monitoring, or occasionally, during low enemy traffic periods, the G-2 would task the RI units for that activity. An indication of the value attached to SIAM unit operations could be the fact that SIAM units often could not get telegraph lines back to their headquarters, so had to rely on radio transmissions encrypted with slow, one-time pads.

It would seem that although the Americans knew that the Germans were able to decipher encodes from the M-209, and knew from ULTRA that the Germans had obtained the U.S. order of battle from tactical intercept, they still did not make monitoring a priority. The Americans were clearly aware of the German's ability to intercept and decrypt U.S. messages, but perhaps they doubted the enemy's ability or willingness to act. The Germans, too, were cognizant of enemy intercept operations, and issued strict edicts to enforce signal security, but still did not field units specifically for friendly monitoring.

Conclusion

Both the German and the American armies came to the Ardennes with a number of handicaps, both in terms of combat capability and signal security. Although many soldiers were inadequately trained and inexperienced, Trevor Dupuy notes, "In devotion to duty, courage,

steadfastness in hardship, and loyalty to country and national traditions, the Germans and Americans were equally matched."[21] Likewise, a comparison between German and American leadership presents a draw: Eisenhower and von Rundstedt, Bradley and Model, Manteuffel and Patton--albeit not without weaknesses, most senior leaders in the offensive were highly competent, and sometimes brilliant.[22] Experts acknowledge, however, that the Germans could never have succeeded in the Ardennes, in spite of great determination and skill, because they simply did not have the resources needed to carry out Hitler's plan.[23] Some German officers hypothesized that if the distribution of forces had been more favorable, the Germans might have been victorious, as signal intelligence gave them complete information on U.S. plans and operations.[24]

No matter the victor, the Ardennes provides a valuable vehicle with which to examine signal security. It serves to illuminate some very interesting differences and similarities between the doctrine and procedures of the two opposing forces. In terms of signal security, the forces were nearly equal. Both armies employed similar devices and procedures, and each suffered from discipline and training lapses which allowed their enemies to gather some potentially very useful information. Each had similar vulnerabilities, although the Germans found great disparities in signal security between American units. The Germans themselves, however, deserve no special praise for their signal security during the offensive, despite the successful early deception. American intercept units easily tracked virtually all the major German combat units throughout the offensive. In retrospect, it seems that the formation of panzer armies and the German "Blitzkrieg" doctrine of swiftness and violence perhaps had led to a force that moved quickly and decisively enough to be blasé about signal security in the offense.

Signal intelligence structures were quite different in the two armies. The German army employed communications experts to build a signal intelligence structure that would exploit

enemy tactical communications to the maximum degree possible. By focusing such efforts at the tactical level, they enabled the tactical commander to have access to timely and relevant intelligence that allowed him to shape his tactical plan. The Americans, by contrast, formed a structure that swept intelligence upward, away from the tactical level, seemingly using enemy intercepts to validate their strategic plans. Although American G-2s at various levels may have certainly put the intelligence gleaned from German intercepts to good use, as they were generally untrained in signal intelligence, they may have also significantly dampened certain positive effects of signal intelligence through misinterpretation or simple negligence. The Germans, however, lost the advantage to the Americans of the mass of contributory detailed information that could not give the field commander "striking and immediate results that he could measure in terms of lives saved, but was of critical importance to overall intelligence."[25]

Allied victories over Axis forces and later, the formation of the Military Intelligence Corps marked the end of an era of U.S. Army Signal Corps involvement in signal intelligence, although the Signal Corps has retained most of the responsibility for U.S Army signal security. The Signal Corps is responsible for transporting the information to the desired point, and the Military Intelligence Corps is responsible for acquiring and analyzing that information. Tactical signal intelligence from such conventional sources such as FM radios continues to play an important role on the battlefield and will ever yield valuable information on the enemy's disposition and intent.

Just as the radio, however, with all its benefits and risks, irrevocably changed the fighting doctrine of every major force, so has the information revolution begun to affect contemporary philosophy on "how to fight." In this age of spy satellites, the Internet and the use of automation to control everything from tank gunsights to global banking, many theorize that information itself has become the object of tomorrow's conflicts. By targeting the computers and

associated databases of municipal utilities, for instance, a determined enemy could reduce entire cities to chaos and effectively destroy the will of a nation. Perhaps in recognition of the tremendously threatening implications of such technology, the U.S. Army has recently introduced a change to its officer personnel management system, which will result in a merged branch called "Information Operations." The new branch will consist primarily of signal and military intelligence officers. Clearly, the U.S Army in the late 1990s is in the midst of another revolution, one which portents to lead the Army, as well as its allies and adversaries, in new directions.

---

[1]Dupuy, 29.

[2]Praun, 140.

[3]Ibid., 141.

[4]Ibid.

[5]Twelfth U.S. Army Group Survey.

[6]Praun, 140.

[7]Praun, 141.

[8]Dupuy, 47.

[9]Woods, 235.

[10]Christopher R. Gabel, "Introduction to Lesson 25. Second Front: Europe, 1944 - 1945." Printed in U.S. Army command and General Staff College, C610 Terms II and III Syllabus/Book of Readings (Fort Leavenworth: USACGSC, December 1996), 274.

[11]Dupuy, 47.

[12]David Kahn, 507.

[13]Kahn, 360.

[14]Raines, 263.

[15]First United States Army, Memorandum No. 4 on the SIGINT situation within First U.S. Army, dated 8 October 1944. NA RG No 457.

[16]Twelfth U.S. Army Group Survey.

[17]Twelfth U.S. Army Group Survey.

[18]The exception to this general appreciation for signal intelligence was Adolf Hitler himself. General Albert Praun writes:

> Only Adolf Hitler, the Supreme commander of the Wehrmacht and Army, withheld his recognition (of the value of signal intelligence) in spite of the tragic blunders he had committed before Moscow, at Stalingrad, and in North Africa, where in each instance he had underestimated the enemy's strength in the face of warnings from communication intelligence. He continued to doubt the reliability of this type of intelligence at a time when it brought him more and more unfavorable, yet undeniable information about the crushing superiority and strategic objectives of his enemies in the West after the Normandy invasion and in the East long before the Baronov offensive was launched in January 1945. By 1944-45 his antagonistic attitude toward communication intelligence reached the point where he forbade the Chief of the Army General Staff and the Chief of the Eastern Intelligence Branch to report the "one-sided and distorted " information based on communication intelligence. On another occasion the Chief of the Eastern Intelligence Branch produced an overwhelming array of indisputable facts drawn chiefly from communication intelligence sources, including accurate data on the enemy's strength, order of battle, and probable moves, as well as his steadily increasing production of tanks and guns. Hitler's reaction to this factual account was the following: "I refuse to acknowledge the appropriateness of this General Staff activity. Only men of genius can recognize the enemy's intentions and draw the proper military conclusions, and such men would never stoop to perform this kind of petty routine." Praun, 239-240.

[19]Ibid., 229.

[20]Twelfth U.S. Army Group Survey.

[21]Dupuy, 370.

[22]Ibid.

[23]Dupuy, 360.

[24]Praun, 141.

[25]"German Operational Intelligence," 28.

APPENDIX A

ORDER OF BATTLE

Allied,16-19 December 1944

Supreme Headquarters Allied Expeditionary Force: SHAEF

SHAEF Reserve:
- 6th British Abn Div
- 11th U.S. AD
- 17th U.S. Abn Div
- XVIII U.S. Abn Corps
- IX U.S. Air Defense Cmd

21st British Army Group:
- XXX Corps
- 29th Ar Bde/11th AD
- First Canadian Army:
  - I British Corps
  - II Corps
    - 51st British ID
      - 6th British Tank Bde
- Second British Army:
  - VIII Corps
  - XII Corps
    - Guards AD
    - 43d ID
    - 53d ID
    - 33d Ar Bde

12th U. S. Army Group:
- Unassigned: 94th ID
- Ninth Army:
  - XIII Corps
    - 84th ID
    - 102d ID
  - XIII Corps Reserve
    - 7th AD (to VIII Corps, 16 Dec)

Ninth Army Reserve:
- 30th ID (to V Corps, 17 Dec)
- XVI Corps (not operational)
  - 75th ID

First U.S. Army:
- VII Corps
  - 104th ID
  - 9th AD
  - 83d ID
  - 5th AD
- VII Corps Reserve
  - 1st ID (to V Corps, 16 Dec)
    - 3d AD (to XVIII Abn Corps, 19 Dec)
- V Corps
  - 8th ID
  - 78th ID
  - 2d ID
  - 99th ID
- V Corps Reserve
  - CCB/9th AD (to VIII Corps, 16 Dec)
- VIII Corps
  - 106th ID
  - 14th Cav Group
  - 28th ID
  - 9th AD
  - 4th ID
- VIII Corps Reserve
  - CCR/9th AD

Third Army:
- XX Corps
  - 90th ID
  - 5th ID
  - 95th ID

XX Corps Reserve
10th AD (to VIII Corps, 17 Dec)
XII Corps
6th AD
35th ID
87th ID
XII Corps Reserve
80th ID (to III Corps, 19 Dec)
Third Army Reserve
III Corps
4th AD
26th AD

6th U.S. Army Group:
Seventh Army:
XV Corps
VI Corps
First French Army:
II Corps
I Corps

German, 16-19 December 1944

Ober Kommand Wehrmacht: OKW

OKW Reserve:
3d PzGrenD
Fuhrer Begleit Bde
Fuhrer Grenadier Bde
167th VGD
150th Pz Bde
Combat Gruppe von der Heydte
10th SS PzD
6th SS MtnD
257th VGD
9th VGD
11th PzD

OB West
Army Group H:
25th Army
LXXXVIII Corps
First Parachute Army
LXXXVI Corps
II Parachute Corps
Army Group B:
15th Army
XII SS Corps
176th ID
59th ID
340th VGD

XII SS Corps Reserve
9th PzD
15th PzGrenD

LXXXI Corps
47th VGD
246th VGD
363d VGD
LXXIV Corps
344th ID
353d ID
85th ID
89th ID

Sixth Panzer Army:
LXVII Corps
272d VGD
326th VGD
I SS Pz Corps
277th VGD
12th VGD
3d FJD
I SS Pz Corps Reserve
12th SS PzD "Hitlerjugend"
1st SS PzD "Liebstandarte Adolf Hitler"
Sixth Panzer Army Reserve:
II SS Pz Corps
2d SS PzD "Das Reich"
9th SS PzD "Hohenstaufen"

Fifth Panzer Army:
LXVI Corps

18th VGD
62d VGD
LVIII Pz Corps
116th PzD
560th VGD
XLVII Pz Corps
2d PzD
26th VGD
XLVII Pz Corps Reserve:
130th Pz Lehr D

Seventh Army:
LXXXV Corps
5th FJD
352d VGD
LXXX Corps
276th VGD
212th VGD
LIII Corps
(no divisions assigned until 21 Dec)

Source: Trevor N. Dupuy, Hitler's Last Gamble (New York: Harper Collins, 1994), 424-456.

APPENDIX B

FIGURES

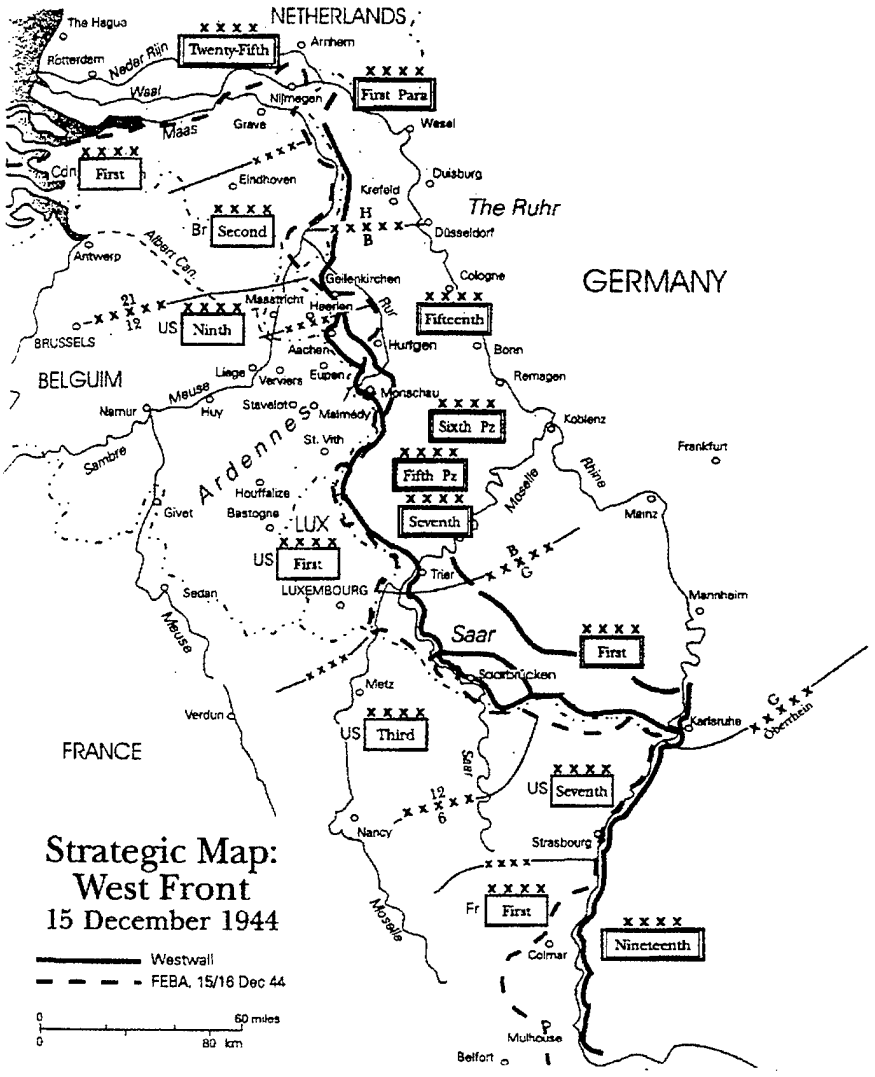

Figure 1. Strategic Map of the Western Front, 15 December, 1944. Source: Trevor N. Dupuy, Hitler's Last Gamble (New York: HarperCollins, 1994), p 7.

Figure 2. Photograph of German Map Illustrating U.S. Order of Battle and Routes of German Attack. Source: Photograph by Dr. Samuel J. Lewis taken at the National Archives, Washington, DC.

ORGANIZATION OF HEADQUARTERS, ARMY SIGNAL SERVICE - 1940

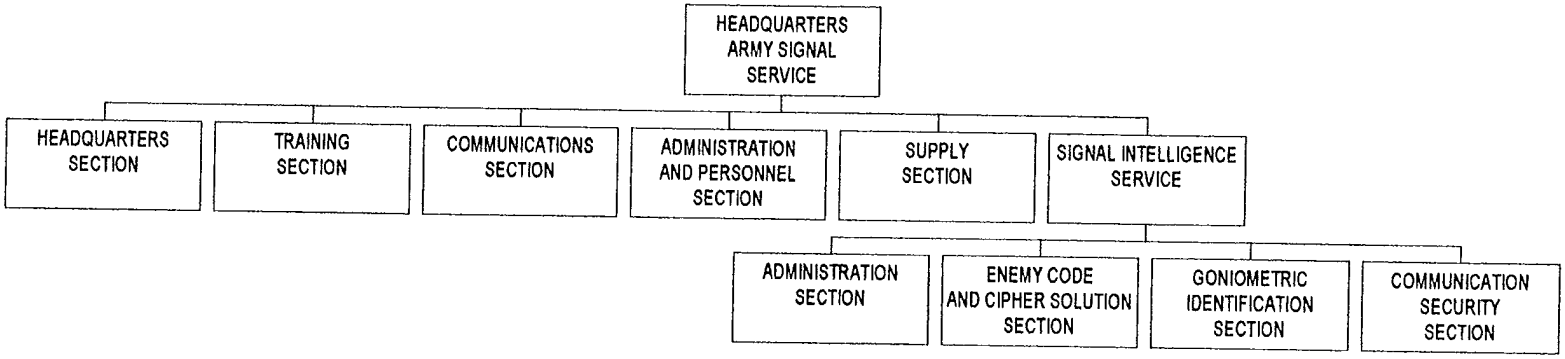

Figure 3. Source: FM 11-20: Signal Corps Field Manual - Organization and Operations in the Corps, Army, Theater of Operations, and GHQ. (Washington, DC: War Department, 1940).

SIGNAL COMPANY, RADIO INTELLIGENCE - 1940

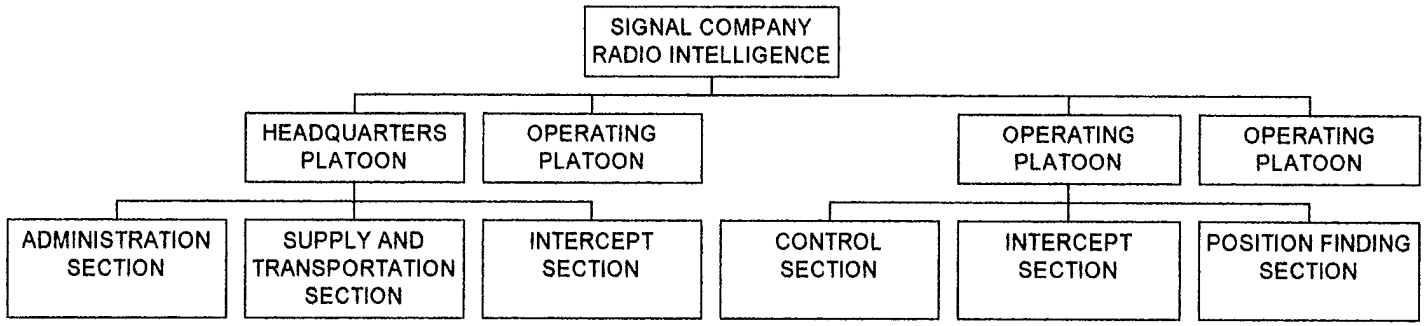

Figure 4. Source: FM 11-20: Signal Corps Field Manual - Organization and Operations in the Corps, Army, Theater of Operations, and GHQ. (Washington, DC: War Department, 1940).

CORPS SIGNAL BATTALION - 1940

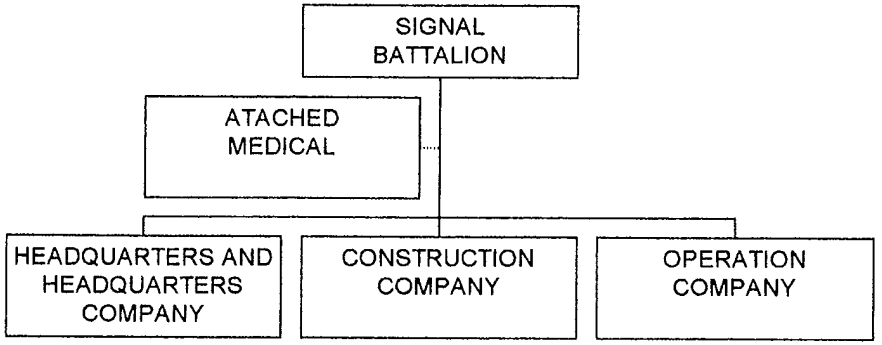

Figure 5. Source: FM 11-20: Signal Corps Field Manual - Organization and Operations in the Corps, Army, Theater of Operations, and GHQ. (Washington, DC: War Department, 1940).

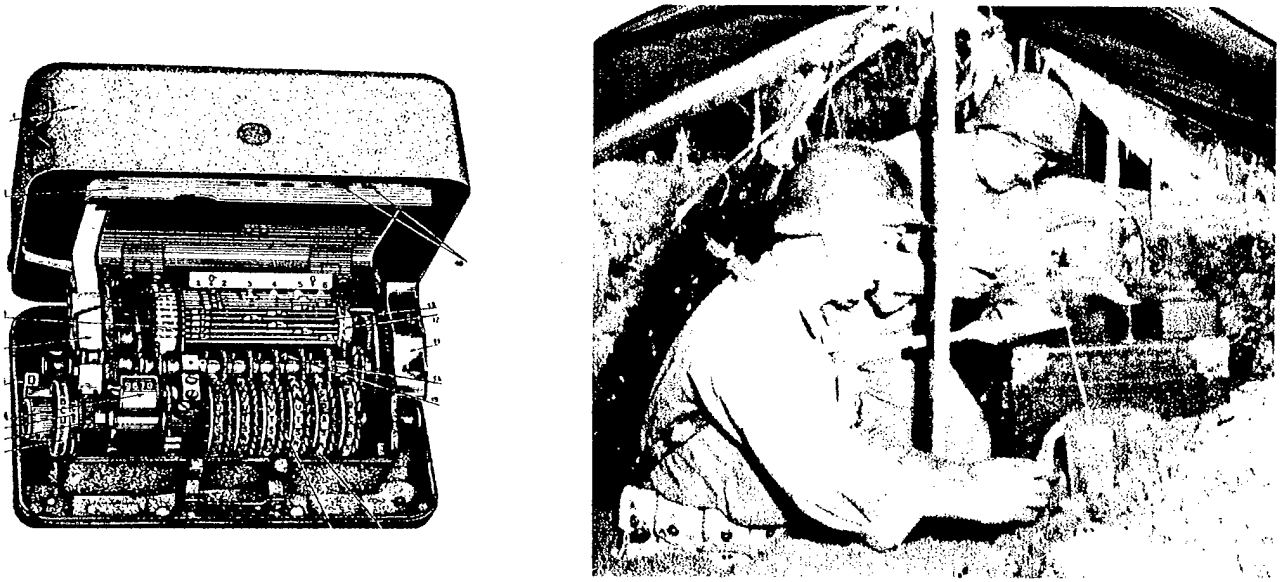

Figure 6. Hagelin's M-209 encryption device (left) and soldiers operating the M-209 in the field (right). Source: David Kahn, The Codebreakers (New York: Scribner, 1996), 429, 847.

FIRST ARMY SIGNAL SERVICE ORGANIZATION - 1944

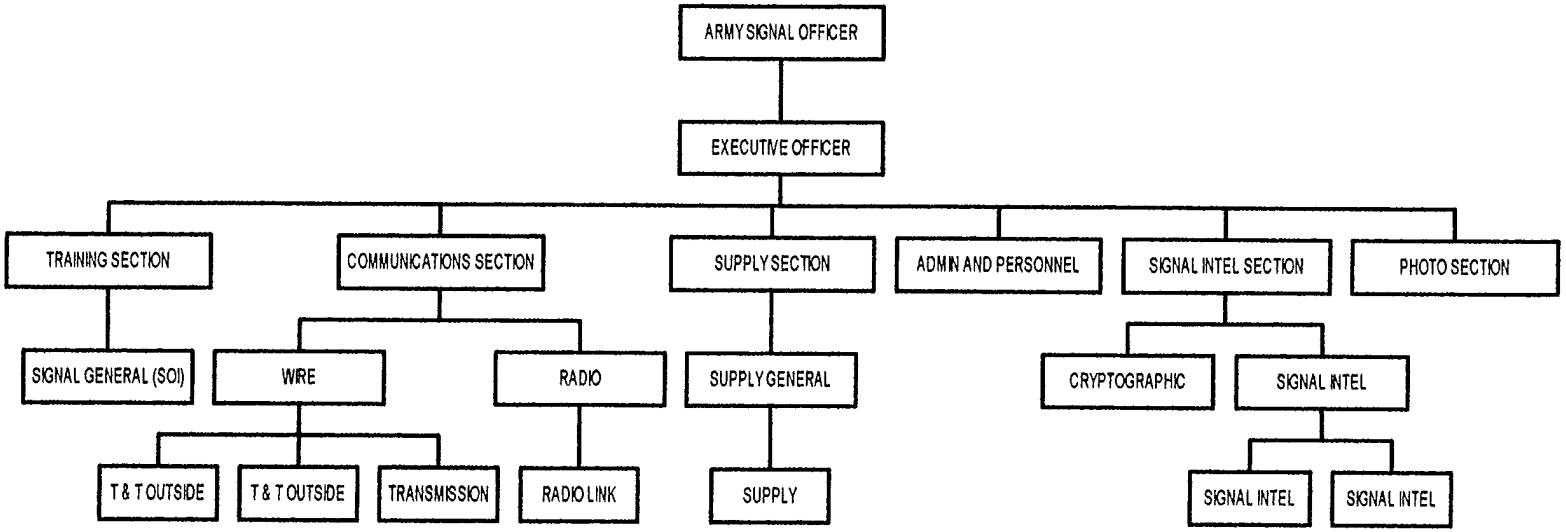

Figure 7. First U.S. Army, "Combat Operations Data," (Governor's Island, New York: Headquarters, First United Sttes Army, 18 November 1946), p 411.

ARMY SIGNAL INFORMATION AND MONITORING SERVICE - 1944

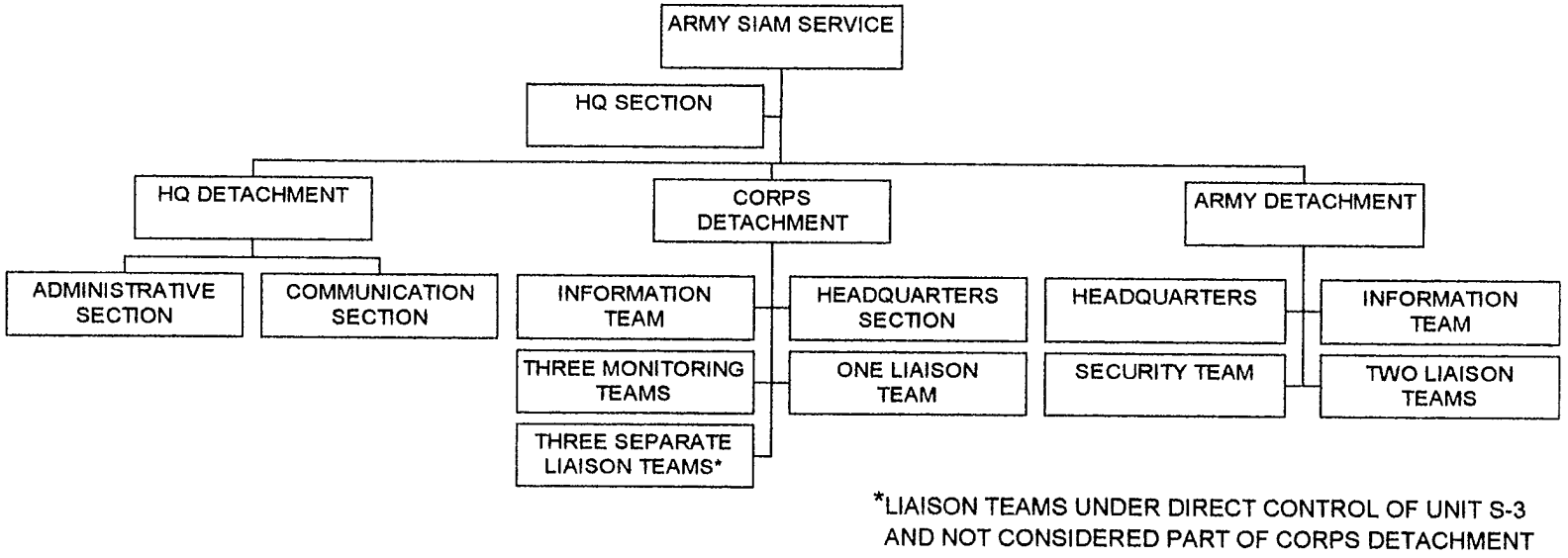

Figure 8. Source: Army Security Agency, Report of Operations of 3325th Signal Information and monitoring company from 15 August 1944 to 1 July 1945," (Washington, DC: Records of the National Security Agency, National Archives Record Group 457, 28 July 1945.)

Figure 9. Photograph of German soldier with messenger pigeons. Source: Len Deighton, Blitzkrieg (New York: Ballantine, 1979), p 74(p).

Figure 10. Photograph of General Guderian in his vehicle with German Enigma Machine. Source: Len Deighton, Blitzkrieg (New York: Ballantine, 1979), p 202(j).

APPENDIX C

12TH ARMY GROUP SIGNAL SECURITY SURVEY - 1945

A 12th Army Group Survey, subject: "The Use of Codes and Ciphers During Critical Operational Period" was conducted after the Offensive. The First US Army, Third US Army, V Corps, VII Corps, XVIII ABN Corps and 99th Infantry Division were asked the following questions:

1. What is the approximate percentage of increase in communications a its maximum during this period?

2. Was equipment such as the M-209 and Slidex strips and cards of sufficient quantities to support the increase in communications?

3. Was there sufficient number of operating cryptographic personnel available to handle the increased communication?

4. Were codes and ciphers in your possession of sufficient quantity and type to handle all necessary communications?

5. Was it necessary to use a standby or emergency code or cipher?

6. Was it necessary to use some other than the authorized codes or ciphers? If so, what were they and how were they used?

7. Comments pro and con on distribution, operational and security problems of the following systems which apply, are requested: SIGABA, M-209, Slidex, PMC, Map Code, Auth Code CCBP0122.

8. Was transmission of classified messages in the clear resorted to? At what unit level was this effected to the greatest extent?

9. What means of transmission was relied upon most - wire lines, radio or message?

10. Was much difficulty encountered in radio transmission?

11. How was transmission security of radio nets controlled? Did the transmission security of the radio nets drop during these critical operational periods?

12. List all agencies of transmission which were available for use.

13. Comments.

Source: Summary of Operational Activity of Detachment D, 12th Army Group, ETO - September 1944-April 1945, RG 457, NA.

SELECTED BIBLIOGRAPHY

Unpublished Works

"Histories of Radio Intelligence Units, European Theater, September 1944 to March 1945." File SRH-228, Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457, 1 February 1946.

"History of the Signal Intelligence Division in ETOUSA." Washington, DC: Records of the National Security Agency, National Archives Records Group No 457.

European Theater of Operations, United States Army. "Signal Operating Instructions Index No 1-20. "ETOUSA, 14 February 1945. (CARL No. 7666-C)

First United States Army. "Basic Records of First U.S. Army Signal Units: 29 May 1945." Washington, DC: Office of the Chief Signal Officer, 29 August 1945.

First United States Army. "Standing Operating Procedures." APO 230: Headquarters, First United States Army, 1 December 1944. (CARL No. 7661)

First United States Army. Memorandum from First Lieutenant Bayard H. Hale, Headquarters, First U.S. Army Signal Service dated 30 November 1944. Subject: Monthly Signal Intelligence Report. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

First United States Army. Memorandum from First Lieutenant Bayard H. Hale, Headquarters, First U.S. Army Signal Service dated 31 December 1944. Subject: Monthly Signal Intelligence Report. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

First United States Army. Memorandum from Major Lawrence D. Summerfield, HQ, First U.S. Army Signal Service, APO 230 dated 27 August 1944 to Signal Officer, HQ, 12th U.S. Army Group, APO 655. Subject: Handling of Information Derived from N/I Traffic. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

First United States Army. Memorandum from Major Lawrence D. Summerfield, HQ, First Army Signal Service, APO 230 dated 13 December 1944. Subject: Signal Intelligence Situation Report. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

First United States Army. "Summary of SIS Activities 2 July 1944 - 1 April 1945." APO 230: Headquarters, First United States Army, 1945. (CARL No. R-11047)

Greiffenberg, Hans von. Military Study P-044a. "Deception and Cover Plans Project No 29." Historical Division, European Command. Konigstein/Taunus, 26 May 1950. (CARL No. N-17570-2)

Kramer, Fritz. Military Study No C-048. "I SS Panzer Corps in the West in 1944." U.S. Army European Command, Historical Division, 1945.

National Archives. "Critical Examination of German Intercept in World War II." Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457. (CARL No N-17570-2)

National Archives. "Safeguarding the Radio Traffic of Signal Units of the 3d Reich, 1944." File SRH-387. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

National Archives. "Report of Operations of 3325th Signal Information and Monitoring Company from 15 August 1944 to 1 July 1945." Washington, DC: Records of the National Security Agency, National Archives Record Group No. 457, 28 July 1945.

Praun, Albert. " Military Study No P-038. "German Radio Intelligence." Washington, DC: Department of the Army, Office of the Chief of Military History, 1950.

Rendulic, _____. "The Element of Surprise." Konigstein/Taunus: Historical Division, European Command, 19 June 1947. (CARL No. N-17236-2)

Twelfth United States Army Group. SRH-048. Survey, Subject: "The Use of Codes and Ciphers During Critical Operational Period." Washington, DC: Records of the National Security Agency, National Archives Record Group No 457, 1945

Twelfth United States Army Group. Memorandum Number 4, dated 8 October 1944, Twelfth U.S. Army Group. Subject: SIGINT Situation within First U.S. Army. Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

Twelfth United States Army Group. Memorandum and note from Major R.E. Button, G-2 Section, Headquarters, 12th Army Group dated 31 December 1944 and 26 October 1944, respectively. Subject: Signal Intelligence Review, 15-25 December 1944. Washington, DC: Records of the National Security Agency, National Archives Records Group No 457.

United States War Department. "A Study of German Operational Intelligence." Washington,DC: War Department, Military Intelligence Division, April 1946. (CARL No. N-13425-18)

United States War Office. "The German Counter-Offensive in the Ardennes: A Study of the Initial Phases." Washington, DC: Directorate of Tactical Investigation, War Diary Section, 18 September 1945. (CARL No N-13205)

Interviews

Moe, Wayne Jerde, Colonel, U.S. Army, Retired. Interview with author, Waynesboro, VA, 4 February 1997.

Schwark, Stuart H., Major, U.S. Army. Interview with author, Fort Leavenworth, KS, on 7 April 1997.

Manuscripts

Dull, Henry L., Sr., "Post-Mortem Writings on the Indications of the Ardennes Offensive, December 1944" Carlisle Barracks, PA: U.S. Army War College, May 1977.

Harley, Jeffrey S. "Reading the Enemy's Mail: Origins and Development of U.S. Army Tactical Radio Intelligence in World War II, European Theater of Operations." Fort Leavenworth, KS, 1993.

Hobar, Basil. "The Ardennes 1944: Intelligence Failure or Cover and Deception Success?" Fort Leavenworth, KS. 1970. (CARL No N-8224.1342)

Horgan, Penelope S. "Signals Intelligence Support to U.S. Military Commanders: Past and Present." Carlisle Barracks, PA: U.S. Army War College, 1991.

Reame, A.G. "Electronic Warfare in the Field Army: A Historical Analysis." Fort Leavenworth, KS: U.S Army Command and General Staff College, 1964.

Published Material

Official Records

First United States Army. "Combat Operations Data." Governor's Island, New York: Headquarters, First United States Army, 18 November 1946.

Third United States Army Signal Intelligence Service. SRH-042. Third Army Radio Intelligence History in the Campaign of Western Europe." Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

Twelfth United States Army Group G-2 Intelligence Branch. "A Study of Operations of G-2 (Intelligence Branch) in the 12th Army Group for the Period 1 August 1944 to 9 May 1945." Headquarters, 12th Army Group, APO 655, July 1945.

Twelfth United States Army Group. SRH-048. "Summary of Operational Activity of Signal Security Detachment 'D,' 12th Army Group ETO, September 1944 - April 1945." SRH-048, Washington, DC: Records of the National Security Agency, National Archives Records Group No. 457.

United States Forces European Theater General Board. " Signal." Study 110- 112, Vol. XXIV, Washington, DC: The War Office, 4 April 1946.

United States War Department, Annual Report to the Chief Signal Officer, Washington DC: 1898.

United States War Department, War of the Rebellion: A Compilation of the Official Records of the Union and Confederate Armies. 128 vols. Washington, DC: Government Printing Office, 1880-1901.

V Corps Historical Section. "V Corps in the ETO, 6 January 1942 - 9 May 1945."

Books

Army Times. A History of the Signal Corps. New York: G P Putnam's Sons, 1961.

Ayres, Leonard P. The War with Germany: A Statistical Summary. Washington, DC: U.S Government Printing Office, 1919.

Barger, Charles J. Communications Equipment of the German Army, 1933-1945. Boulder, CO: Paladin Press, 1989.

Behrendt, Hans-Otto. Rommels Kenntnis vom Feind im Afrikafeldzug. Freiburg: Rombach, 1980.

Brown, J. Willard. The Signal Corps, USA in the War of the Rebellion. Boston: U.S. Veteran Signal Corps Association, 1896.

Clayton, Aileen. The Enemy is Listening, New York: Ballantine Books, 1982.

Cole, Hugh M. The Ardennes: Battle of the Bulge. Washington, DC: U.S. Army Center of Military History, 1993.

Deavours, Cipher A., and Louis Kruh. Machine Cryptography and Modem Cryptanalysis. Dedham, MA: Artech House, 1985.

Dupuy, Trevor N. Hitler's Last Gamble. New York: Harper Collins, 1994.

Finnegan, John Patrick. Military Intelligence: A Picture History. Arlington, VA: History Office, U.S. Army Intelligence and Security Command, 1984.

Gilbert, James L., and John P Finnegan. U.S. Army Signals Intelligence in World War II. Washington, DC: U.S. Army Center of Military History, 1993.

Glantz, David. Soviet Military Deception in the Second World War. London: Frank Cass, 1989.

Horne, Alistair, and David Montgomery. Monty: The Lonely Leader, 1944-1945. London: MacMillan, 1994.

Kahn, David. The Codebreakers. New York: Scribner, 1996.

Kirkpatrick, Charles E. An Unknown Future and a Doubtful Present: Writing the Victory Plan of 1941. Washington, DC: Center of Military History, United States Army, 1990.

Liddell Hart, B.H. The German Generals Talk. New York: Quill, 1979.

MacDonald, Charles B. The Battle of the Bulge. London: Weidenfeld and Nocolson,1984.

MacDonald, John. Great Battles of World War II. New York: MacMillan, 1986.

Marshall, Max L. The Story of the U.S. Army Signal Corps. New York: Franklin Watts, Inc, 1965.

Raines, Rebecca Robbins. Getting the Message Through: A Branch History of the U.S. Army Signal Corps. Washington, DC: U. S. Army Center of Military History, 1995.

Schramm, Percy Ernst. "The Preparations for the German Offensive in the Ardennes (Sep - 16 Dec 1944)," in World War II German Military Studies, Volume 10. Edited by Donald S. Detweiler. New York: Garland, 1979.

Smith, Bradley F. The Ultra-Magic Deals. Novato, CA: Presidio Press, 1992.

Sorley, Lewis. Thunderbolt. New York: Simon and Schuster, 1992.

Terrett, Dulany. The Signal Corps: The Emergency. Washington, DC: Office of the Chief of Military History, Department of the Army, 1956.

Thompson, George Raynor and Harris, Dixie R. The Signal Corps: The Outcome. Washington, DC: Office of the Chief of Military History, United States Army, 1966.

van Crevald, Martin. Command in War. Cambridge: Harvard University Press, 1985.

Winterbotham, F.W. The Ultra Secret. New York: Dell, 1974.

Winton, John. Ultra in the Pacific. Annapolis, MD: Naval Institute Press, 1993.

Woods, David L. A History of Tactical Communications Techniques. Orlando, FL: Martin Marietta, 1965.

Articles

Gabel, Christopher R. "Introduction to Lesson 25. Second Front: Europe, 1944 - 1945." Printed in U.S. Army command and General Staff College, C610 Terms II and III Syllabus/Book of Readings. Fort Leavenworth: USACGSC, December 1996.

Holder, L. D., and Edwin J. Arnold. "Moving the Heavy Division." Military Review (July 1988): 35-39.

Taylor, Blaine. "A Combat History of the lst SS Panzer Division," in Hitler's Army: The Evolution and Structure of German forces, 1933 - 1945. San Luis Obispo: Command, 1995.

Field Manuals

U.S. Army. FM 11-20: Signal Corps Field Manual - Organization and 0perations in the Corps, Army, Theater of Operations, and GHQ. Washington, DC: War Department, 1940.

_____. FM 11-22: Signal Operations in the Corps and Army. Washington, DC: War Department, 1945.

_____. FM 11-10: Signal Corps Field Manual - Organization and Operations in the Infantry Division. Washington, DC: War Department, 1941.

_____. FM 100-5: Operations. Washington, DC: U.S. Government Printing Office, 1986.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   Fort Leavenworth, KS 66027-6900

2. Defense Technical Information Center
   Cameron Station
   Alexandria, VA 22314

3. Major Michael J. Farley
   Center for Army Tactics
   USACGSC
   Fort Leavenworth, KS 66027-6900

4. Dr. Samuel J. Lewis
   Combat Studies Institute
   USACGSC
   Fort Leavenworth, KS 66027-6900

5. LTC Nancy Morales
   Center for Army Tactics
   USACGSC
   Fort Leavenworth, KS 66027-6900

6. Major Michael S. Bell
   3517 Remington Lane
   Leavenworth, KS 66048

7. Commander
   U.S. Army Signal Center and Fort Gordon
   ATTN: Command Historian
   Fort Gordon, GA 30908

8. Commander
   U.S. Army Intelligence Center and School
   ATTN: Command Historian
   Fort Huachuca, AZ 85613

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 6 /June /1997

2. Thesis Author: Major Laurie G. Moe Buckhout

3. Thesis Title: Signal Security in the Ardennes Offensive: 1944-1945

4. Thesis Committee Members

Signatures: Michael J. Harvey
Samuel [illegible]
Nancy A. Morales

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S----------SAMPLE--------SAMPLE----------SAMPLE-----------SAMPLE-----------S			
A	Limitation Justification Statement /	Chapter/Section /	Page(s) A
M			M
P	Direct Military Support (10) /	Chapter 3 /	12 P
L	Critical Technology (3) /	Sect. 4 /	31 L
E	Administrative Operational Use (7) /	Chapter 2 /	13-32 E
---------SAMPLE---------SAMPLE----------SAMPLE-----------SAMPLE----------			

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Pages(s)
	/	/
	/	/
	/	/
	/	/

7. MMAS Thesis Author's Signature: Laurie Moe Buckhout

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).